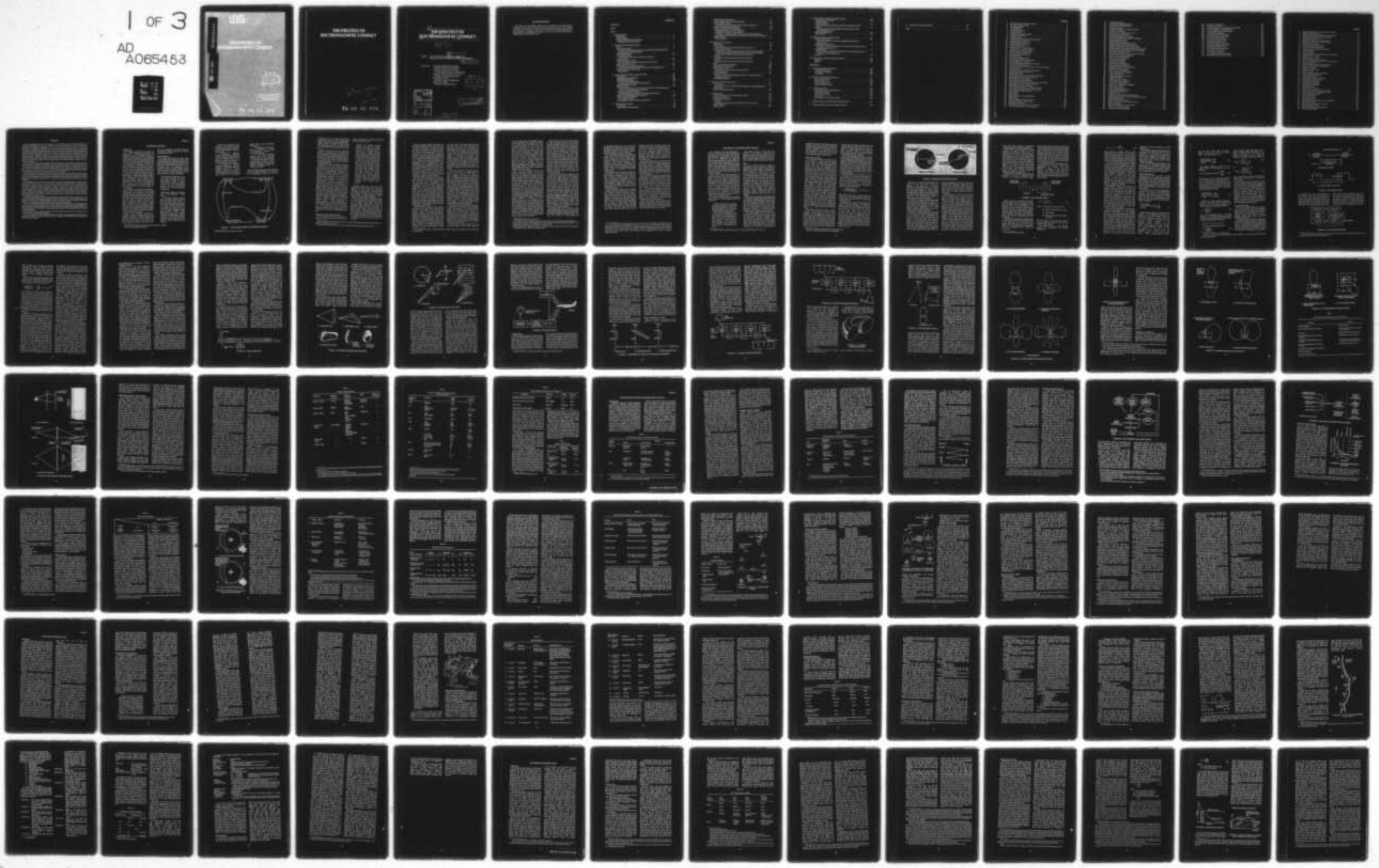
AD-A065 453 AIR FORCE ACADEMY COLO F/G 17/4
THE STRATEGY OF ELECTROMAGNETIC CONFLICT, (U)
FEB 79 R E FITTS

UNCLASSIFIED NL

1 OF 3
AD
A065453



THE STRATEGY OF ELECTROMAGNETIC CONFLICT

THE STRATEGY OF ELECTROMAGNETIC CONFLICT

AD - C005551

ok use - per letter

AIR FORCE Academy, Colo

Feb. 79

79 02 23 079

(6)

THE STRATEGY OF ELECTROMAGNETIC CONFLICT

(12) 286p.

(10)

EDITOR LIEUTENANT COLONEL RICHARD E. FITTS
ASSOCIATE PROFESSOR OF ELECTRICAL ENGINEERING

313 671

(11) Feb 79

Contributors: Lieutenant Colonel Robert W. Burton
Professor of Electrical Engineering
Lieutenant Colonel Frank L. Cloutier
Assistant Professor of Electrical Engineering
Lieutenant Colonel Clarence S. Summers, Jr.
Instructor of Electrical Engineering
Major Elliott R. Brown
Instructor of Electrical Engineering
Major John A. Zingg
Instructor of Computer Science

011 550

ACKNOWLEDGEMENT

The editor and contributors express sincere gratitude to the many persons throughout the Department of Defense who have taken time from their busy schedules to review previous editions of this book and offer their very helpful suggestions. We also specifically acknowledge the support of the Air Force Avionics Laboratory, Wright-Patterson Air Force Base, Ohio.

CONTENTS

APPENDICES

FIGURES

TABLES

PREFACE

This text originally grew out of a desire by certain faculty members of the Department of Electrical Engineering of the United States Air Force Academy to relate the classroom instruction in Electrical Engineering to the real Air Force world which the cadets would encounter after graduation. Initially it concerned itself mostly with ECM techniques as embodied in particular pieces of equipment. However, over the course of years faculty members performing research and consultation in the field of the strategy of electronic warfare became associated with this text and its classroom instruction. From that marriage arose the realization that the important issues in electronic warfare today are not so much what, but why? and how much? And the average cadet is more likely to have to address the latter questions in his career as an Air Force officer than the former. So the present text has evolved toward a broader view of electronic warfare.

About the same time it became evident that this broader concept of electronic warfare was not well understood throughout the military services. Electronic warfare has long been concerned with particular techniques to defeat particular equipment. But electronic warfare does not exist in a vacuum, there are other ways of accomplishing the same objectives, and electronic warfare must compete with all of these. Thus we need a good understanding of the broader concepts of electronic warfare so that we can properly evaluate its usefulness.

From this reasoning it appeared that such an approach would also be valuable to the electronic warfare staff officer, especially if he were newly assigned. Traditionally one has learned electronic warfare by proceeding from the particular to the general. But a staff officer should have a diverse background in warfare so that he can fit in context the general concepts and then particularize them later.

As we attempted to write down these broader concepts, we gradually came to realize the fact that electronic warfare is not "electronic" in the common usage of that term, for there are large quantities of avionics which do not concern electronic warfare, such as an aircraft autopilot, or an inertial navigation system. Electronic warfare is jargon for conflict carried out using electromagnetic energy as the battleground. And these broader issues really become strategic and tactical principles to be observed in this conflict. Because electronic warfare conveys an image of highly sophisticated technology to many of its practitioners we decided that it would be much more appropriate to title this book consistent with its content, and also more to the point of our first objective, the typical cadet.

To ask typical students to learn technical details before learning broad concepts is to risk permanently losing his interest in electronic warfare, especially if he is not science oriented. We desired to show him that electromagnetic energy is a sphere of conflict which can have great impact on any military operation for which he may become responsible.

Thus we have chosen to introduce him to the overall picture first and fill in the details later. In this way we trust we will prepare him in the best possible way for his future career, whether it be as an Electronic Warfare Officer, a crew member associated with Electronic Warfare Officers, a staff member planning operations involving electronic warfare, or the commander of a unit using electronic warfare.

As a result this text is written with this varied audience in mind. How well it meets the needs of both we leave to the reader's judgment.

Any views expressed in this book are those of the authors. They should not be interpreted as reflecting the views of the United States Air Force Academy or the official opinion or policy of any governmental agency.

ELECTRONIC WARFARE

Introduction

The purpose of this text is to make you aware of the capabilities, limitations and applications of the diversified science of electronic warfare. Unfortunately electronic warfare is not electronic, it is not conducted using electrons; but it is electromagnetic and it uses as its battleground the total spectrum of electromagnetic radiation. Granted that this radiation is usually generated by "electronic" equipment, the converse is definitely not true, that all electronic equipment is involved in this conflict. However, the advent of new, modern weapons systems seems to correspond to progressively greater reliance upon victory in this electromagnetic conflict as a prerequisite for victory in battle. Hence every commander must understand the principles involved in this silent and invisible battle so he can turn it to his advantage; he must understand the effects this battle can have on his weapons so he can manage it to his advantage.

It is this silent and unseen electromagnetic conflict that is the subject of this book. Traditionally, this conflict has been called electronic warfare. Although clarity might be somewhat advanced by using a more descriptive term, we would lose in communication with the myriad of people who speak the jargon of electronic warfare. And in a field where specialized terms abound, adding another is not a mark of distinction. Hence we will use the term electronic warfare for the most part, reserving electromagnetic conflict for those cases where we wish to emphasize the true nature of the conflict.

Much of the information pertaining to electronic warfare is classified and can be expected to remain so. A great portion of this classified information is very detailed and thus beyond the scope of this survey. The basic principles, however, are easily derived and are unclassified. We shall therefore concentrate on basic principles and leave the details for later study.

Basic Definitions

For many years there has been wide misunderstanding of electronic warfare (EW) and its purpose. Part of this problem stemmed from the classified nature of the subject, but a large part of the difficulty has been due to a confusing variety of definitions of the common terms in electronic warfare. Recognizing this problem, the Joint Chiefs of Staff issued a policy in 1969 defining the basic terms, definitions which we will adopt.

> "ELECTRONIC WARFARE is military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum.[1]
>
> THERE ARE THREE DIVISIONS OF ELECTRONIC WARFARE....
>
> 1. *Electronic Warfare Support Measures*[2] (ESM) is that division of EW involving actions taken to search for, intercept, locate, record, and analyze radiated electromagnetic energy, for the purpose of exploiting such radiations in support of military operations. Thus, ESM provides a source of EW information required to conduct *electronic countermeasures* (ECM), *electronic counter-countermeasures* (ECCM), threat detection, warning, avoidance, target acquisition, and homing.

[1] Some workers in the field now call this Electromagnetic Warfare (EMW).

[2] Italics in this quote added by the editor.

2. ECM is that division of EW involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. ECM includes:

a. *Jamming*—the deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy.

b. *Deception*—the deliberate radiation, reradiation, alteration, *absorption, or reflection* of electromagnetic energy in a manner intended to mislead the enemy in the interpretation or use of information received by his electronic systems. There are two categories of deception.

(1) *Manipulative*—the alteration or simulation of friendly electromagnetic radiations to accomplish deception.

(2) *Imitative*—introducing radiation into enemy channels which imitates his own emissions.

3. ECCM is that division of EW involving actions taken to insure friendly effective use of the electromagnetic spectrum despite the enemy's use of EW."[3]

These definitions emphasize that electronic warfare is really dependent on the radiation of electromagnetic energy and not on

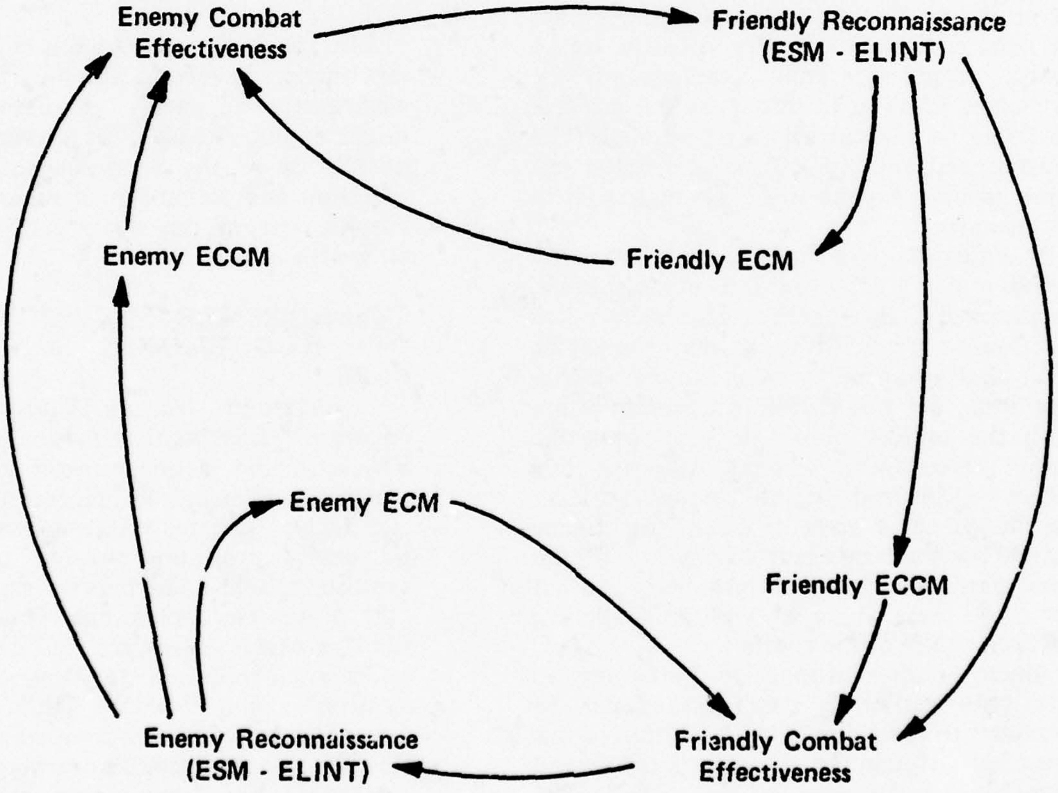

Enemy Combat Effectiveness
Friendly Reconnaissance (ESM - ELINT)
Enemy ECCM
Friendly ECM
Enemy ECM
Friendly ECCM
Enemy Reconnaissance (ESM - ELINT)
Friendly Combat Effectiveness

FIGURE 1. THE INTERACTIONS OF ELECTRONIC WARFARE

[3] Extracted from JCS Memorandum of Policy 95.

"electronics" *per se*. Hence EW includes systems using all forms of electromagnetic energy (e.g. radio, radar, infrared (IR), optical systems, lasers, etc.) with one major exception. Radiation produced by nuclear weapons is usually classed as nuclear effects and not EW.

Another term often used in electronic warfare is *penetration aids* or *penaids*. This term includes all techniques or devices used to insure the survival of an attacking aircraft as it penetrates a hostile defense system on its way to its target and return. Usually ECM is included in penaids, in fact the two are often used interchangeably.

Although it is not an officially sanctioned definiton, we often see electronic warfare discussed in terms of active and passive roles.[4] *Passive electronic warfare* is the search for and analysis of electromagnetic radiations to determine existence, source and pertinent characterisitcs of the enemy's use of the electromagnetic spectrum. *Active electronic warfare* is the radiation or reradiation of electromagnetic waves so as to impair the enemy's use of electronic equipment, or to mislead the enemy in the interpretation of data received from his electronic devices. In general, ESM is passive electronic warfare, ECM is active electronic warfare, and ECCM may be either. But the distinctions may not be clear cut, for ESM may involve actively radiating a signal to determine the characteristics of the enemy equipment and ECM may require a passive reception of the enemy signals in order to decide what signal to counter. Figure 1 shows graphically the relationships between ESM, ECM, ECCM and the order of battle. It is apparent that EW is not a static encounter but a dynamic interaction between two opposing forces. The following bit of history will illustrate this fact.

Examples of Early Electronic Warfare

One of the first leaders in World War II to recognize electronic warfare as a vital phase of military operations was Winston Churchill. In his war memoirs he said:

> "During the human struggle between the British and German Air Forces, between pilot and pilot, between A. A. batteries and aircraft, between ruthless bombing and fortitude of the British people, another conflict was going on, step by step, month by month. This was a secret war, whose battles were lost or won unknown to the public, and only with difficulty comprehended, even now, to those outside the small high scientific circles concerned. Unless British science had proven superior to German, and unless its strange, sinister resources had been effectively brought to bear in the struggle for survival, we might well have been defeated, and defeated, destroyed."[5]

Churchill called this secret war "The Wizard War" and we know it as "Electronic Warfare". In the quote he was specifically referring to activities which occurred during the bombing of Britain by the Luftwaffe. These made an ardent electronic warfare supporter of Britain's Prime Minister.

The Battle of the Beams. Churchill referred to the first employment of electronic warfare as "The Battle of the Beams" which took place in England during 1940. In order to accomplish their bombing of Britain, the Germans established an extensive series of radio stations (200 KHz - 900 KHz) in northern France. These stations were beamed over London. An aircraft equipped with a loop antenna could get on any of these beams and follow it directly over London. Primarily a navigational aid, this system was known as "Lorenz".

[4] This is a different use of active and passive than commonly encountered in Electrical Engineering, and also is different from active and passive ECM.

[5] Winston S. Churchill, *Their Finest Hour*. (Boston: Houghton Mifflin Company, 1949), pp 381-2.

Except for going in VFR[6] this was the only system the German bombers had. There was no inertial navigation, no airborne radar navigation and no Loran. So, after considerable study, the British countered Lorenz with a system known as "Meaconing" which was designed to actually bend the navigational beams. A meacon (masking beacon) consisted of a receiver and transmitter separated by 5 to 10 miles. The receivers intercepted the navigational beams and relayed them to the transmitters for retransmission. · Hence, German bombers attempting to obtain bearings received signals from both the Lorenz transmitters and the meacons. This countermeasure was apparently very effective since on several occasions German crews became so completely confused and disoriented that they actually landed at British air bases.

When it became obvious to the Germans that Lorenz was being effectively countered, they switched to a new system. Two intercommunicating transmitters were established on the French coast; while one transmitted dots, the other transmitted dashes. Since the two beams were transmitted parallel to one another, an aircraft flying a course directly between the beams received a solid tone and any deviation from the prescribed course resulted in the reception of either dots or dashes. The width of the solid tone was such that it enabled the German bombers to determine their position over the target within approximately 800 yards. This "Knickebein" (crooked leg) system was called "Headache" by the British.

The British had a choice of two countermeasures to this system. They could jam the receivers in the bombers, in which case the Germans would most likely immediately abandon Headache, or the British could use deception, strengthening one side of the without the Germans knowing it. They chose deception, and strengthening one side of the beam with transmitters so that it was literally bent. Whimsically, this countermeasure was called "Aspirin". The British had excellent intelligence concerning the Headache system and were able to put Aspirin into operation the very first time the Germans used Headache. For the next two months the British had the Germans so confused that very few bombs were dropped on the assigned targets. There is a story that during these two months of Headache being dosed with Aspirin, no one had the courage to tell Goering that his beams were being twisted. Goering thought the beams were infallible, and anyone who cast doubt on them would be eliminated. The German air crews suspected that the beams were being mauled but, naturally enough, did not voice their suspicions.

In the fall of 1940 the Germans initiated the use of "Ruffian", a propaganda transmitter which operated 24 hours a day. Propaganda was normally transmitted from a nondirectional antenna; however, just prior to a raid the transmitter switched to a directional antenna and beamed its transmission over the selected target area. In addition, the Germans used another narrow beam which crossed the propaganda beam to mark the bomb release point. The discovery of this bombing system can be credited to the people of London. They noticed that if they were listening to the propaganda broadcast and their radios became increasingly louder a raid would invariably follow. The radios of those listening outside London would become weaker prior to a raid. Consistent reports from people in and around London soon revealed Ruffian's primary function.

The countermeasure to Ruffian was known as "Bromide". It consisted of retransmission of the propaganda on the same frequency making the navigational aid useless. The British also used directional antennas to rebroadcast the beam in such a manner that the bomb loads were dropped in the channel. The British press credited the erratic German bomb drops to evasive action against British Spitfires to keep the Germans in ignorance of the success of Bromide.

At this point in the "Wizard War" the Germans evidently became quite distressed

[6] Visual Flight Rules: flight in visual meterological conditions (VMC)–clear of clouds and in visual contract with the ground.

over the effectiveness of the British countermeasures program. They equipped one squadron, "Kampf Gruppe 100" with all of the available navigational aids. The various aids were used alternately in order to reach the target. Once these aircraft reached the target they dropped incendiaries to visually mark the target for the following formations. This system was first used on November 14, 1940 to bomb Coventry. The initial countermeasures used by the British consisted of decoy fires called "Starfish". After the KG-100 squadron had dropped its incendiaries large numbers of Starfish were ignited in open spaces about the target, resulting in a dispersal of the bomb load.

One of the last schemes devised by the Germans was called "Benito". At this time frequency modulation (FM) was not common, and the Germans assumed that the British would probably not be monitoring FM. (Sadly enough, they were right.) As a result, portable FM stations along the bombing route in France and England were established by strategically located agents who actually talked the pilots in over London. To the dissatisfaction of the Germans, however, the British were not outdone and they eventually intercepted the transmission and countered very effectively by using a skilled linguist who transmitted false orders to the German pilots on the original FM frequency. This countermeasure, known as "Domino", was so effective that some of the German pilots became disoriented to such a degree that they were forced to land in England. Benito was used until June 1941. The success of Domino as a countermeasure is evident from the bitter remarks heard passing between the bombers and their controlling ground stations. The bombing of Dublin on the night of May 30–31, 1941, may have been an unforseen and unintended result of Domino.[7]

Jamming. The first case of British jamming of radio channels occurred in the Libyan campaign during November, 1941. The British had not used communications jamming prior to this time because of their fear of retaliation by the Germans. However, a decision was made to jam the German tank communications operating from 27 MHz to 33.5 MHz. The jamming equipment compared with modern standards was very crude, but it did the job. If you can imagine tank formations with no means of intertank communications, you have a clear picture of the success of the electronic warfare operation. However, there was one fault in the British tactics; they neglected to provide fighter protection for the airborne jammers and consequently the jamming was soon brought to an abrupt halt by German fighters.

During this same period, the British were being seriously hampered in moving shipping through the English channel. The Germans had accurate, radar-controlled, coastal guns located on the Continent side of the Channel. This situation led the British to construct ground jammers, which effectively countered these German radars. However, the tables were turned when the Germans moved the Scharnhorst from Brest through the Channel to the North Sea. During this classic electronic warfare operation, every British radar was completely jammed but one, and the British did not believe that one.[8] Even though life of the Scharnhorst was prolonged, the British learned a profitable lesson. The effectiveness of radar jamming was proven and, in addition, the Germans had tipped their hand as to their capabilities.

One might ask–why was there no large scale jamming prior to this time? The answer is that after the initial use of a countermeasure its effectiveness greatly decreases; because once used, it is then an open target for

[7] Churchill, *The Finest Hour*, pp 381–389.

[8] The following two references give the account of this operation from both the German and British sides.

Captain Helmuth Giessler, "The Breakthrough of the 'Scharnhorst'–Some Radio Technical Details.", *IRE Transactions on Military Electronics* MIL-5: 2–7 (January 1961).

Sir Robert Watson-Watt, "Battle Scars of Military Electronics–The Scharnhorst Breakthrough", *IRE Transactions on Military Electronics*, MIL-1: 19–25 (March 1957) counter-countermeasures, or it may be used by the enemy to neutralize our own weapons. The British, especially, were fearful that the deleterious effects of the enemy reaction would outweigh the benefits of jamming.

The United States had observed, with keen interest, this battle between offensive electronic systems and the countermeasures techniques employed to reduce their effectiveness. It had become apparent future operations would become increasingly dependent upon electronic warning and control systems. Also, it was quite obvious that these systems would be susceptible to electronic warfare action.

The Spring of 1942 welcomed to England a small number of research personnel from the US who were designated to work with the RAF radiation countermeasures program. From this embryonic organization, a laboratory specifically designated to work on countermeasures design was established in 1943 at Malvern England. The work of these individuals early in 1943 produced the first US designed jammer.

After the Battle of Britain came the Battle of Berlin where the British began to combat the German defensive weapons instead of their offensive weapons. The main German defensive weapons were the Junkers 88, Heinkel 219, and the Messerschmitt 110 night fighters. To provide the eyes for these fighters were two very fine ground radars. The Freya radar operated on approximately 120 MHz and the Wurzburg radar on approximately 570 MHz, a very high frequency for those days. The Freya gave longer range but the Wurzburg radar had excellent precision and resolution. A common mode of operation was to use the Wurzburg to provide guidance control to a "master" searchlight. As soon as the master searchlight located the raiding bombers, other lights would be able to illuminate the targets. Once the targets were illuminated the night fighters would move in for visual attack.

Before the British designed and built radar jammers they wanted to know more about the radar's ability to combat jamming. So they acquired one in a brilliant commando raid (a tactic the Israelis also used in 1969). They were pleased to discover no specific anti-jamming circuitry in the Wurzburg radar other than that it was capable of being tuned over a wide range.

One of the most effective countermeasures against these two radars was the use of chaff or "window" as the British called it. The British were very reluctant to use it against the Germans, however, because they were afraid that the Germans would find the pieces of aluminum, discover the principle themselves and use it against the British. So . . . until the British developed some sort of defense against it they refused to use it and hence compromise it. Electronic jamming was also used, but its greatest effectiveness was against the ground-to-air communications links so that the radars could not pass information to the night fighters.[9]

From these harried, and sometimes even desperate, beginnings evolved the massive efforts in electronic warfare such that today a substantial percentage of our defense budget is spent on EW in one form or another.

[9] A very interesting history from another point of view is found in the following book: Alexander I. Pali, *Technik und Methoden des funkelektronischen Krieges*, trans. Lt Col Gernot Padur (East Berlin: Deutscher Militärverlag, 1968), pp 294—237. This book is available in English translation to government users from Defense Documentation Center, Cameron Station, Alexandria, VA, 22314 as AD 860660L and to civil users from the Commander, Army Foreign Science and Technology Center, Washington, D.C. 20315 as document FSTC-HT-23-470-69.

Chapter 2

THE PRIMARY ELECTROMAGNETIC THREATS

It is apparent from the definitions in Chapter 1 that electronic warfare combats all the systems of an adversary which radiate electromagnetic energy. Clearly, our first step must be to understand the significant operating characteristics of these systems. We can generally divide these systems into two classes: sensors and communications equipment; and we observe that by far the greatest effort in elctronic warfare is devoted to the first class. The reasons for this emphasis will become clear as we develop the concepts of electronic warfare.

Most of the sensors which comprise the electronic threat to Air Force operations are found in air (and space) defense systems. These systems have many components of both threat classes which we might profitably investigate but the most pervasive sensor is radar. If we can deny the enemy the effective use of his radars, we attain a strategic and tactical advantage because we deny him the eyes and ears of his offense and defense. Conversely, the existence of electronic-warfare-resistant military radars has become a *sine qua non* of military power.

The truth of this fact is not lost on military planners today. A recent magazine article had this to say.

> "[The] Soviet Union is making substantial progress in developing and deploying military radar as an essential corollary of its emergence as a world-wide military power.
>
> The Russians apparently have embraced the new maxim that he who controls the electromagnetic spectrum controls the outcome of any conflict in modern war or global politics. They understand and appreciate the essential role radar plays in fulfilling this dictum."[1]

For these reasons we shall spend the majority of our effort on radar and the electronic warfare activities related to radar. Before we launch into a detailed discussion of these electronic threats, however, we want to make a short detour to the subject of noise.

Noise

In much of what follows we shall be discussing electronic signals and systems as though they existed without contamination. This common practice allows clear exposition, but it tends to conceal one of the fundamental realities of electronics–noise. It is a fundamental fact of electronic systems that there will always be some noise present. If nothing else, the fact that we are not operating at absolute zero temperature (0°K) guarantees that there will be random electron motion in our electronic components. Electron movement constitutes current and this random current through any resistance produces a "noise" voltage in the system. All electronic systems, especially radar, are ultimately limited by the amount of noise present.

The existence of noise has two implications for electronic systems. First, noise determines the minimum signal amplitude that can exist in the system, for if the signal is much smaller than the ever-present noise it is lost. Thus noise determines the limit upon the performance of many systems, among them radar. Electronic warfare is a conflict between systems which are ultimately noise limited.

The second implication concerns the nature of electronic warfare. By its very nature electronic warfare involves interfering with the adversary's electronic systems. Such interference is commonly done with electric signals–what signals are best to use? Although many specialized signals exist it should be clear that a noise-like signal is almost always effective, for no system is proof against its

[1] Barry Miller, "Soviet Radar Expertise Expands", *Aviation Week 94* (February 15, 1971): 14.

ravages. Thus much of electronic warfare is a discussion of the effects of artificial noise-like signals on electronic equipment. In addition, a common standard for comparison is the noise-like signal. Consequently, noise lurks in the background of the rest of this book always ready to make itself manifest.

Basic Radar Principles

The concept of distance measurement by echo timing is so much a part of contemporary science, especially military-oriented science, that it is sometimes difficult to believe that radar is a relatively recent invention. The reflection characteristics of radio energy have been known from the time of Hertz (1886), but it was not until the 1930s that anyone measured the round trip travel time of that energy. As a result radar is a very young science, yet a science that was nearly full grown when it was born! Although there were many other contributors, the outstanding prophet who deserves to be called the "Father of Radar" was Sir Robert Watson-Watt. In 1932 he was asked by the Royal Academy of Britain if a radio ray could be directed as a weapon against an enemy aircraft. He answered the question by saying, in effect, "No, but we certainly can locate the aircraft." His answer is the now famous "Death Ray Memo" in which he proposed an air defense *system* before anyone had built the first radar *set*. In addition, he was able to forsee many aspects of our modern air defense networks. Much of the subsequent radar development has been the putting of the flesh on the skeleton described by Watson-Watt.[2]

Pulse Radar. The basic principle of radar[3] is range measurement by echo timing. Suppose you are standing in the bow of a rowboat on a very foggy day. You know that somewhere ahead, there is a cliff. So you cup your hands like a megaphone and shout toward the cliff. Now you begin counting the number of seconds. After 5 seconds, you hear the echo. Since sound travels at roughly 1000 feet per second, you know that your voice has traveled about 5000 feet. Therefore the cliff is approximately 2500 feet away. This, of course, is a crude measurement; you have a rough idea of the distance to the cliff and only a general idea of the direction. Nevertheless, you have approximated almost all of the functions of a radar set.

One major difference between an actual radar and our leather-lunged sailor is the use of electromagnetic energy instead of sound energy. This difference dictates many other changes in the system, but the general idea of measuring range by echo timing remains the same. When we use electromagnetic energy travelling at the speed of light, we get a whole new time reference, because the speed of light is approximately one million times as fast as the speed of sound.

The Radar Mile. Let us compute how long it would take for a burst of radar energy (a *radar pulse*) to travel from the radar to a target, be reflected, and return to the radar set. The speed of light is 3 x 10^8 meters/sec and one nautical mile is 1853 meters. Therefore the round trip time to and from a target 1 nautical mile away is:

$$t = \frac{2(1853)\text{ meters}}{3 \times 10^8 \text{ meters/sec}} = 12.35\ \mu\text{sec} \quad (1)$$

This time, 12.35 μsec, is often defined as a "radar mile". The reflection from a target 100 nautical miles away would return to the radar set in 1235 μsec.

Indicators. How can we measure this time interval? With an oscilloscope the process is almost trivial. Refer to Figure 2a and imagine the sweep starting on the left hand side of the scope face at time zero and moving to the right. After 1235 μsec the returning echo arrives and causes the moving dot on the scope to displaced upward. Knowing the sweep speed of the dot, we can measure the time delay of the echo and thus derive the distance to the target. If we want to save ourselves computational labor, we can calibrate the sweep so we can read off the distance directly. This scope display is often called an *A-scope*.

[2] The memo is reproduced in Appendix D for the reader's interest.

[3] Radar is an acronym for Radio Detection And Ranging.

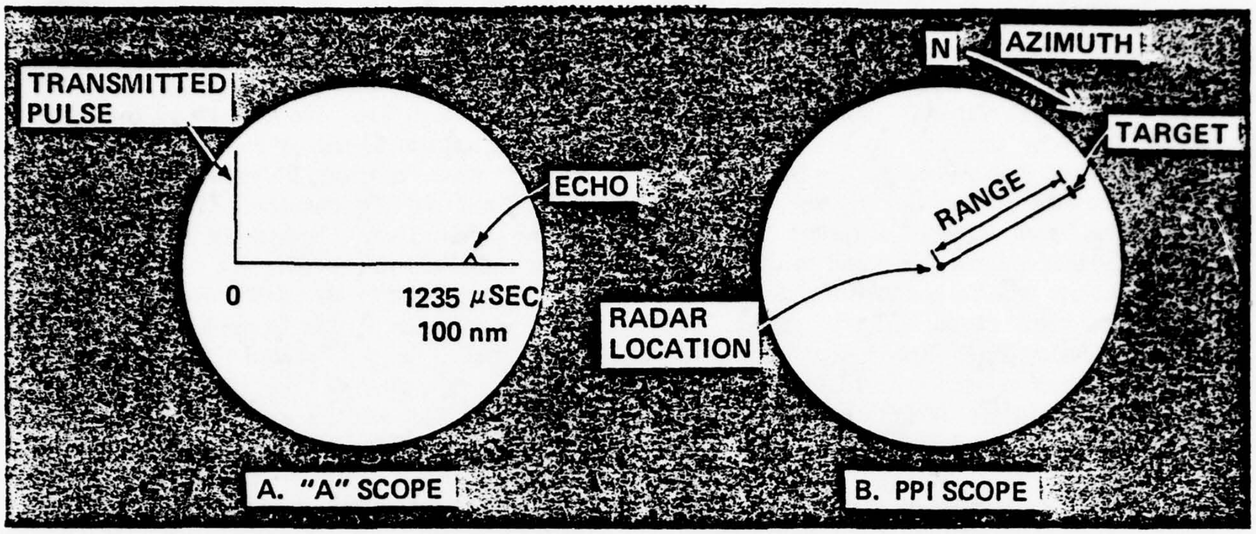


FIGURE 2. TWO BASIC RADAR INDICATORS

Thus far we can measure the distance to a target, but we often want to know the azimuth of the target also. A common method of measuring azimuth is to confine the transmitted energy to a narrow beam through antenna design. By slowly rotating the antenna (and thus the beam) in azimuthwe can determine the target azimuth because we know it is the direction the antenna is pointing when the echo is strongest.

Now that we have both azimuth and range we can plot the location of our target on a map. But plotting is laborious business if we must measure the azimuth and the range separately. The development of the *plan position indicator* (PPI) allows us to let the radar do the plotting automatically.

Suppose we arrange to have the sweep start in the center of our oscilloscope rather than at the left-hand side. Furthermore we cause the sweep, which now goes from the center to the outer edge of the scope, to rotate in synchronism with the antenna. Finally, instead of deflecting the sweep when the echo is received we cause the echo to make the sweep brighter (*intensity modulation*). Now our target appears as a bright spot at the correct azimuth and range relative to the radar location at the center of the scope (Figure 2b). This display is called a *PPI scope* and the radar with the rotating antenna a *search* radar. If we were to place a transparent map over the scope we could locate the target with respect to other features natural or man-made.

Range Resolution. So far we have assumed that our transmitter can radiate very short pulses of energy. What happens when we increase the length of the radiated pulse? If we have only one target the measurement is the same as before. But suppose we have two targets the same azimuth; if they are close together, then their echos will overlap and we will be unable to separate them. This problem is called the problem of *range resolution*, the inability to distinguish targets which are closer together than the distance equivalent to the length of the radar pulse. The obvious solution to this problem is to use short pulses, but if we make the pulses too short, they contain so little energy we cannot detect them. (Noise begins to rear its ugly head.) We can make the pulses stronger to compensate for their shortness, but eventually we are limited by the capability of our transmitter.

Thus radar design becomes a compromise between a number of conflicting demands.

FM-CW Radar. Given the problem of range resolution it appears useless to use a transmitter that transmits continuously, a *CW radar,* for now we have no basis for timing. But suppose that we cause the frequency of the transmitter to vary linearly with time. The echo will now have a different frequency from the transmitted signal and the difference in frequency will be proportional to the echo delay, or the range to the target. This *FM-CW radar* finds application principally in such areas as radio altimeters and police radar; we mention it because it forms the background for the doppler radar.

Doppler Radar. The Doppler principle was discovered in 1842 by Christian Johann Doppler. It was originally thought to apply only to sound waves until astronomers found that the light spectrum from heavenly bodies moving away from the earth was different than the spectrum from heavenly bodies moving toward earth. We now know that the principle applies whenever energy is transmitted by wave motion between two points moving relative to each other. The frequency of the received wave is directly proportional to the radial closure speed.

You may have observed the doppler effect while waiting for a train to pass. As the train approached and passed you, you detected a change in the frequency (pitch) of the whistle. If the train were stationary and you had driven by it, you would also have heard a frequency different from that which was being transmitted by the train's whistle.

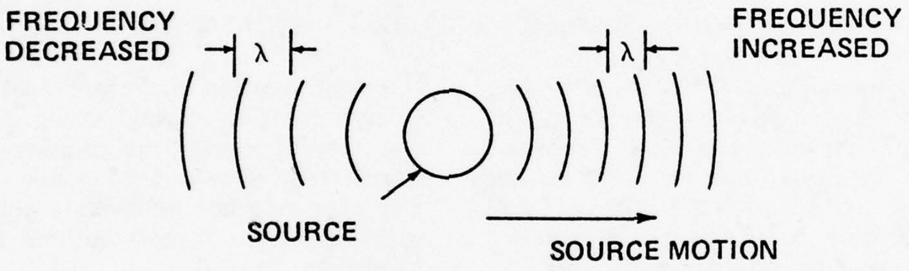


FIGURE 3. THE DOPPLER EFFECT

Figure 3 shows a moving source of either sound or radio energy. As the source moves, the wavelength (λ) is compressed in the direction of travel and expanded in the opposite direction. Therefore, an observer in front of the source would detect a higher frequency (more cycles per second) while an observer behind the source would detect a lower frequency. The same effect will take place if the observer is moving and the source is stationary.

For radar, the energy makes a round trip to the target. Since the receiver is usually located in the same spot as the transmitter, two doppler shifts take place, and the relative velocity in the standard doppler relationship[4] must be multiplied by a factor of two. Hence

$$f_r = \frac{C \pm 2V_t}{C} f_t \qquad (2)$$

Where f_r = frequency received by radar

f_t = frequency transmitted by radar

C = speed of light

V_t = relative motion between target and radar

The plus sign is used when the target is moving toward the radar and the minus sign when it is moving away.

The doopler shift, f_d, is the difference between the transmitted and received frequencies.

[4] See any standard physics textbook.

$$f_d = f_r - f_t = \frac{\pm 2V_t}{C} f_t \qquad (3)$$

The amount of doppler shift at radar frequencies is about 30 Hz per 100 MHz of the transmitted frequency per 100 knots of relative movement. Hence, a radar transmitting at 10 GHz and flying at 300 knots would measure a maximum doppler shift of 9,000 Hz.

If we use the CW radar mentioned above and keep the transmitted frequency constant we find that we have a doppler radar, one that measures relative velocity but not range. On the other hand the FM-CW radar responds to both range and relative velocity, thus we need some additional information to determine either range or velocity. (In the radar altimeter it is assumed that the relative velocity is small so that the frequency difference is due only to range—that is altitude.) This interdependence of range and velocity is usually expressed as the range-velocity *ambiguity* of the radar.

Pulse-Doppler Radar. Our discussion of doppler radar has assumed that the radar transmits continuously—can we apply the doppler idea to a pulse radar? Yes we can, but to do so we must preserve a sample of the transmitted frequency so that we can compare it with the echo received some time later. This requirement for frequency comparison after the radar pulse has been transmitted does place some restrictions on the components of the radar set as we shall see, but it does allow the radar to gain more information about the target.

There are two approaches to the frequency comparison requirement. A *moving-target indicator* (MTI) radar uses the doppler information to differentiate between moving and non-moving targets. This is typically done with a *delay-line canceller* which compares two successive echoes by subtraction. A stationary target will have the same range and doppler shift on successive pulses and so it will cancel out, but a moving target will differ either in range or doppler shift and so it will be passed by the canceller. Unfortunately, the price for MTI is some loss in receiver sensitivity due to the canceller, and the presence of *blind speeds*, non-zero radial velocities for which the delay-line canceller output is zero.

The normal meaning of *pulse-doppler* radar is a radar which produces accurate velocity information. In this case, the velocity is obtained by measuring the doppler shift. These radars typically use high *pulse repetition frequency* (PRF)—they transmit many pulses per second—so that they have small unambiguous range.

Such a pulse-doppler radar will have *blind ranges* due to second-time-around (and multiple-time around) returns coinciding with the transmitted pulse. Thus in both cases the desire to measure both range and velocity with a single radar results in a compromise.

Radar Range Equation.

Basic to all use of radar is some understanding of the factors that affect the performance of the radar. We have discussed the concepts of the radar mile and doppler shift, but how far away can the target be seen by the radar? This question is answered by the radar range equation which relates all the major factors pertinent to receiving an echo from a target.

If the power of the radar transmitter is denoted by P_t and if an omnidirectional antenna is used (that is, one that radiates uniformly in all directions) the power density (power per unit area) at a distance R from the radar is equal to the transmitter power divided by the surface area of an imaginary sphere of radius R.

$$\left.\begin{array}{l}\text{Power density}\\ \text{from omnidirectional}\\ \text{antenna}\end{array}\right\} = \frac{P_t}{4\pi R^2} \qquad (4)$$

Radars usually employ directive antennas, instead of omnidirectional antennas, to channel most of the radiated power P_t into some particular direction. The gain G_t of an antenna is a measure of the increased power radiated in the preferred direction compared with the power that would have been radiated from an omnidirectional antenna. It may be defined as the ratio of the maximum power density from the subject antenna to the power density from a lossless omnidirectional antenna with the same power input. The power density at the target from an antenna with a transmitting gain G_t is

$$\left.\begin{array}{l}\text{Power density}\\\text{from directive}\\\text{antenna}\end{array}\right\} = \frac{P_t G_t}{4\pi R^2} \tag{5}$$

The target intercepts a portion of the radiated power and reradiates it in all directions.

$$\text{Power reradiated by target} = \frac{P_t G_t \sigma}{4\pi R^2} \tag{6}$$

The parameter σ is the "radar cross section" of the target and has the dimensions of area. It is a characteristic of the target and is a measure of its size as seen by the radar. The power density in the echo signal at the radar receiving antenna (assuming it is collocated with the transmitter) is then

$$\left.\begin{array}{l}\text{Power density}\\\text{of echo signal}\\\text{at radar}\end{array}\right\} = \frac{P_t G_t \sigma}{(4\pi R^2)^2} \tag{7}$$

Finally the radar antenna captures a portion of the echo power. If the effective capture area of the receiving antenna is A_r, the echo power P_r received at the radar is

$$P_r = \frac{P_t G_t A_r \sigma}{(4\pi R^2)^2} \tag{8}$$

This is the fundamental form of the radar equation. If a common antenna is used for both transmission and reception (as is usually the case), antenna theory states that

$G_t = G_r = G$ and $A_r = A_r = A$[5]

Using these relationships we have:

$$P_r = \frac{P_t G A \sigma}{(4\pi R^2)^2} \tag{9}$$

The maximum radar range R_{max} is the distance beyond which the target can no longer be detected. It occurs when the received echo signal P_r just equals the minimum detectable signal S_{min}. Therefore

$$S_{min} = \frac{P_t G A \sigma}{(4\pi R^2{}_{max})^2} \tag{10}$$

or

$$R_{max} = \sqrt[4]{\frac{P_t G A \sigma}{(4\pi)^2 S_{min}}} \tag{11}$$

S_{min} is the equivalent noise level at the input of the radar receiver, about 10^{-14} watts for a typical radar.

Even though the range equation contains the major factors influencing the range it is often observed that actual range performance is much less than the equation predicts. In part this is the result of many other factors which we have ignored in writing the equation. Typically, none of these factors is large but their cumulative effect can considerably reduce the maximum range. In addition, there are many operational factors which also produce effective performance decrease. Many of these operational factors will be discussed later in this book.

A Typical Pulse Radar

Now that we have sketched the different types of radar and the two basic principles that they use let us consider a pulse radar in more detail. Since the purpose of radar is to transmit and receive a pulse of electromagnetic energy a good place to start our discussion is the pulse.

The Radar Pulse. Consider the transmitted waveform of a pulse radar shown in Figure 4a. By way of the figure we have defined three terms: (1) The *pulse width* (PW) which is the amount of time that the transmitter is "on", (2) the *pulse repetition time* (PRT)[6] which is the time from the beginning of one pulse to

[5] Also $G\lambda^2 = 4\pi A$ where λ is the wavelength.

[6] The PRT is the inverse of the *pulse repetition frequency* (PRF). It is also commonly called the *pulse repetition interval* (PRI).

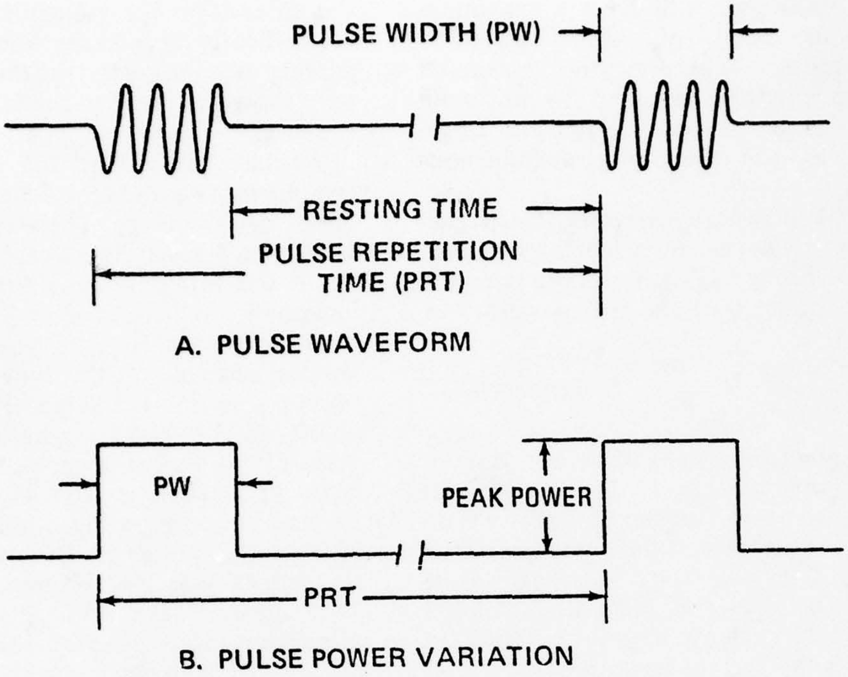


FIGURE 4. THE RADAR PULSE

the beginning of the next, and (3) the *resting time* which is the time the transmitter is "off". If the receiver shares the same antenna with the transmitter, radar echoes can only be received during the resting time. The resting time then becomes the maximum echo delay that can be observed since an echo that arrives much later becomes associated with the following pulse and appears at a range much less than its true value. The range limit imposed by the PRT is called the *maximum unambiguous range*[7] and echoes from ranges greater than that value are called *second time around* returns. As an example, a radar with a

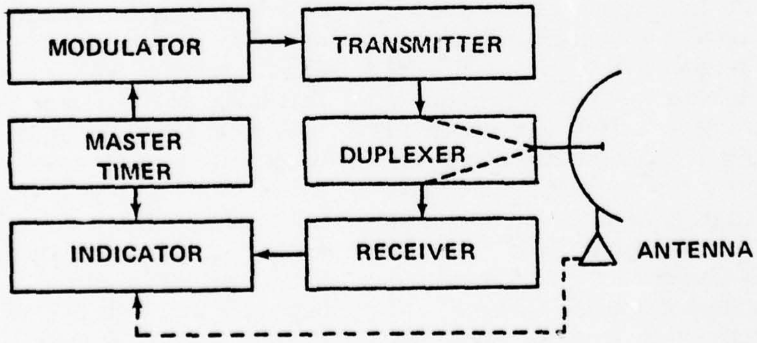


FIGURE 5. A PULSE RADAR SYSTEM

[7] Since the pulse width is usually less than one percent of the resting time, the maximum unambiguous range can be related directly to the PRT with negligible error.

PRT of 3000 μsec will have a maximum unambiguous range of 3000/12.35 = 243 nautical miles. Typically, the maximum unambiguous range is less than the maximum range in order to assure reliable target detection at the maximum unambiguous range.

Let's look at basically the same figure again except that the ordinate is labeled in watts. (Figure 4b) From this figure we can compute the average power from the peak power.

$$\frac{\text{Average Power}}{\text{Peak Power}} = \frac{\text{PW}}{\text{PRT}} = \text{duty cycle} \qquad (12)$$

It is convenient to assign a name to this ratio. We call this the *duty cycle*, and it represents the ratio of the time that the transmitter is on compared to one cycle of the operation of the transmitter. A typical search radar might have a pulse width of 6 μsec and a PRT of 3000 μsec. The duty cycle then would be 0.002. In other words the average power would be only 0.2% of the peak power. It is because of this convenient happenstance that we can have multimegawatt radar sets with equipment that has only tens of kilowatts average power capability.

Transmitter. The heart of any radar set is the *master timer* (Figure 5). Basically it is an astable multivibrator which generates one timing pulse (trigger) for each radar pulse we wish to transmit. The trigger goes to the modulator which delivers a very large pulse of DC voltage to the transmitter. During this DC pulse the transmitter puts out its high energy pulse of radio frequency energy, which goes through the duplexer to the antenna and is radiated. The duplexer serves as a switch so that the transmitted pulse travels only to the antenna and not to the receiver. At the same time that the trigger goes to the modulator, it also goes to the indicator. This tells the indicator, "We are sending our transmitted pulse out now. Start measuring the time until the receiver tells you that an echo has returned." The echo is picked up by the antenna and routed back through the duplexer to the receiver. From there the detected and amplified echo is sent to the indicator where it is displayed. The line from the antenna to the indicator is to show that the indicator also keeps track of where the antenna is pointing so that the display will not only show the range to the target but also the azimuth.

We have seen that the purpose of the *transmitter* is to deliver a series of high energy bursts of RF energy. There are basically two ways that this can be accomplished. Historically it was first done by starting with a small, low-power oscillator and amplifying the signal until it was as large as possible. With the triodes available at the time the maximum output was not too large. Then the British developed the cavity *magnetron* in the early 1940s. With a magnetron, which is basically a diode in a magnetic field, it is not necessary to have a string of amplifiers. When the high-voltage pulse of DC is applied to a magnetron, it is shocked into oscillation at a high power level. The output of the magnetron is connected directly to the antenna, eliminating the need for intermediate amplifiers. Because a magnetron is shocked into oscillation periodically, there is no guarantee that it will oscillate at exactly the same frequency each time but three decades of development have done much to reduce this inherent instability. The utter simplicity of the device and the elimination of the need for RF driving stages, makes the magnetron popular for airborne applications where weight and space are at a premium.

The development of the *klystron* amplifier dictated a return to the "string of amplifiers" approach for many radar applications. The chief advantage of the klystron amplifier is that it is capable of large, stable output power with good efficiency and high gain. Because it is basically a power amplifier, it can be driven by a stable, crystal-controlled oscillator followed by a frequency multiplier chain thus facilitating doppler measurements. The chief limitations of klystrons are their relatively large size and high operating voltages. Large size, of course, is better suited to ground installations. High power klystrons require DC potentials of greater than 100 Kv, necessitating special high-voltage handling techniques. High voltage produces X-ray radiation in the vicinity of the tube, so that lead shielding must be provided to protect operating personnel.

Perhaps one of the most impressive klystrons was one of the first. In March of 1949 Stanford University had a klystron operating at 2900 MHz with a pulse width of 2μsec. The peak power was 30 megawatts! The Eitel-McCullough Corporation produced a klystron for the BMEWS radars that puts out an average power of 75 Kw. The tube is over 10 ft tall and weights 800 pounds. The tube is surrounded by 2 tons of lead for shielding purposes. On the other hand klystrons for very high frequency radars can be smaller than a package of cigaretts.

In a klystron-type radar we must have a separate oscillator to provide the RF sinusoid. Actually the basic oscillator may be operating at a fairly low frequency, and the use of frequency multiplier stages will bring the frequency up to the desired range. This type of transmitter is called a master-oscillator power-amplifier (MOPA) transmitter.

The *modulator* is a major portion of any pulsed radar. The job of the modulator is to provide an extremely large, very short pulse of DC voltage to the transmitter. This is similar to the requirements of the ignition system of an automobile but the requirements are much more stringent. To accomplish this we need an energy storage device and a switch. Between the pulses (i.e. during the resting time of the transmitter) energy is accumulated and stored in the storage device. Then by means of a switch all of this energy is "dumped" into the transmitter in the form of a pulse. It is not an easy job to create a well-shaped pulse of short duration and greater than 100 kilovolts in amplitude.

The *duplexer* is required when both the transmitter and the receiver use the same antenna. It is basically a switch which connects the transmitter to the antenna when it is producing a radar pulse and then removes the transmitter and connects the receiver at all other times. The main requirements that the duplexer must satisfy are low loss and isolation. Low loss is desirable on transmit both because power lost in the duplexer does not detect targets and because that power must be dissipated as heat. On reception, power loss effectively raises the minimum detectable signal and thus decreases the radar range. Isolation relates the amount of transmitter power that appears at the receiver when the transmitter is on. That power must be small enough to not saturate the receiver or burn out any sensitive components in it.

Receiver. As important as the transmitter is the radar receiver. The ability of a radar receiver to detect the presence of the echo and extract information from it is fundamentally limited by the presence of noise. Noise can enter the receiver via the antenna along with the desired signal (external noise), or it may be generated within the receiver itself (internal noise). Although noise can never be completely eliminated, it must be minimized if optimum radar performance is to be obtained. Noise and its elimination are probably the most important considerations in the design of sensitive receivers used with modern radars. Good noise immunity tends to make the radar more resistant to ECM also. (See Chapter 6.)

The primary receiver design considerations in addition to noise and sensitivity are gain, dynamic range, bandwidth, tuning, ruggedness and simplicity. Together these requirements constitute the tradeoffs or compromises that must be made in any radar receiver design.

The total power *gain* of a receiver must be sufficient to amplify the minimum detectable signal to a level that will be seen on the indicator. Given a minimum detectable signal of approximately 10^{-14} watts it is easy to see that gains of from 10^{10} to 10^{15} are not uncommon. At the same time we do not want a strong echo from a nearby target to saturate the receiver. Thus the reciever must have wide *dynamic range*, it must be able to handle both strong and weak signals without changing its response.

The receiver *bandwidth* must be wide enough to encompass the frequency spectrum of the transmitted signal plus any doppler frequency shift which might occur. You may not be surprised to learn that the bandwidth is usually chosen to be the reciprocal of the pulse width, but the frequency response of the receiver is not simply a matter of bandwidth. The transmitted pulse can be thought of in terms of its frequency spectrum (as obtained from its Fourier transform). In other words it consists of a unique set of sinusoids at many different frequencies, each frequency component having its own distinct amplitude and phase. The optimum radar receiver will attempt to capitalize on this fact by having the response characteristics of the receiver exactly match the spectrum of the expected echo. This is the so-called "matched filter" approach that pervades radar receiver design.

Tuning is usually not as important a requirement in radar receivers as it is in communication receivers. The receiver tuning range need be no greater than that of the transmitter, and since it is more difficult to tune a high power transmitter than a receiver, tuning is seldom a limitation in receiver design. However, radar transmitters, especially self-excited oscillators, tend to drift in frequency and some means of automatic tuning must be incorporated into the receiver to keep it in step with the uncontrolled frequency variations of the transmitter. This technique is called *automatic frequency control* (AFC).

Ruggedness and *simplicity* become important design parameters, even more important than in normal commercial practice, because military radars are likely to be deployed in remote areas and maintained by relatively inexperienced personnel. Poor maintenance is usually reflected by a slow degradation of performance, thus ruggedness and simplicity of design have an indirect but important effect on the basic performance of the radar.

By far the most common form of radar receiver is the superheterodyne receiver, shown in Figure 6. The echo signal enters the system via the antenna and duplexer. It is then amplified by the low noise RF amplifier. When external noise is negligible, the noise generated by the input stage of the receiver determines the receiver sensitivity. In the diagram, the input stage is an RF amplifier, but in many practical radar receivers, the RF amplifier is dispensed with and the mixer acts as the first stage. The function of the mixer stage is to translate the RF frequency to a lower intermediate frequency (IF), usually 30 or 60 MHz. This is accomplished by heterodyning the RF signal with a local oscillator in a nonlinear element (mixer) and extracting the signal component at the difference frequency. The frequency is translated to IF where the necessary gain is easier to obtain than at RF. The detector, which is usually a crystal diode or diodes, extracts the video modulation from the IF. These echo pulses are then amplified in the video stages to a level high enough to operate the indicator or display devices.

Although there are other possibilities, most displays are based on the cathode ray tube. A great deal of flexibility to exists in the colors, size, duration and geometry of displays, but the two portrayed in Figure 2 are probably the most common.

Antenna. The radar antenna has two basic functions: (1) to efficiently launch and receive electromagnetic energy into the atmosphere or space, and (2) to direct the energy into an appropriately shaped beam. (From antenna theory it can be shown that the antenna is able to receive energy in the same proportion as it is able to transmit energy; that is, the transmitting and receiving "beams" are identical.) The shape of the

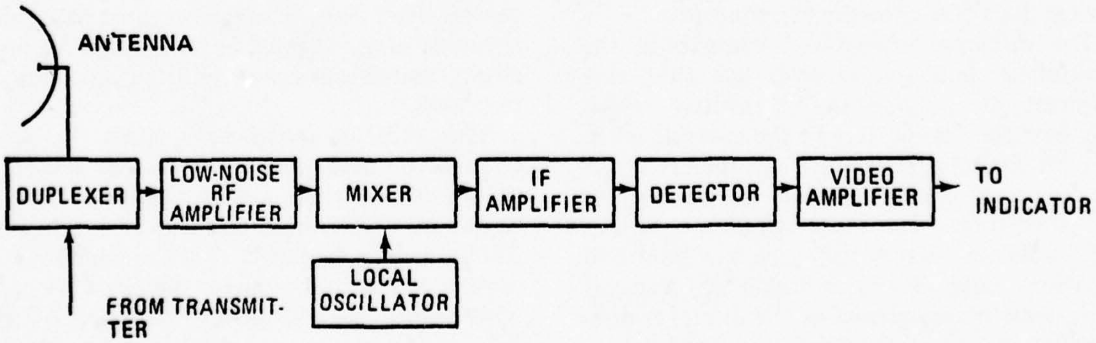


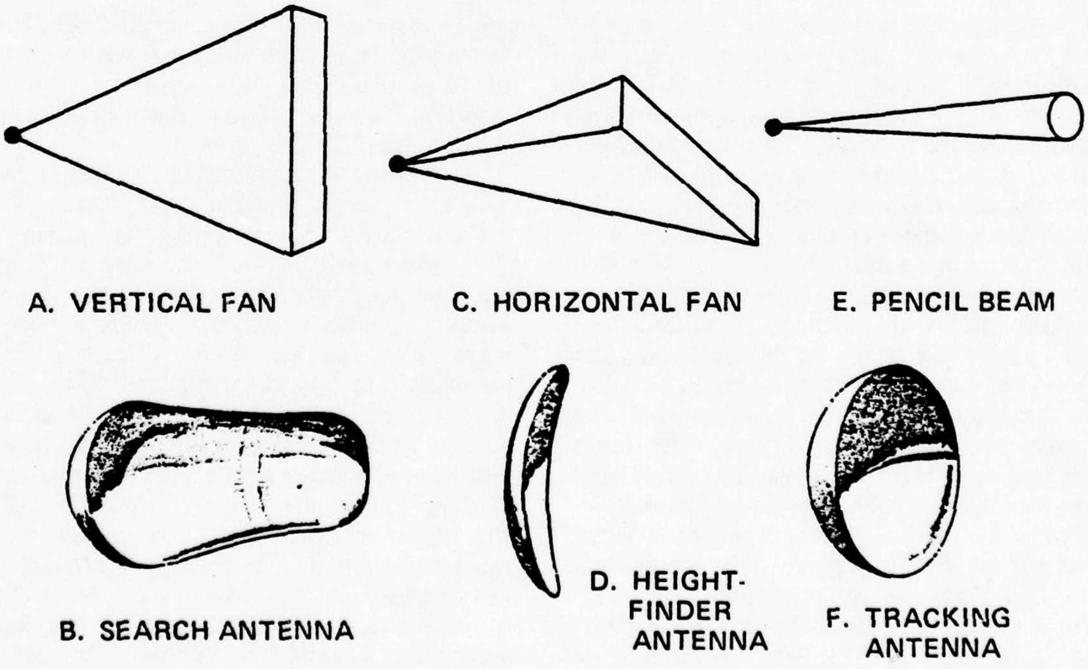
FIGURE 6. A RADAR RECEIVER

beam of radar energy, its *antenna pattern,* depends upon the purpose of the radar. For a search radar we need to measure range and azimuth but not height. Therefore the shape of the beam would be as seen in Figure 7a. We would like the beam to be as narrow as possible to give good azimuth resolution. One or two degrees is a practical beam width. The beam height often is about 30° to 35°. We shape this beam using a basically parabolic reflector following the optical laws that would apply to search lights. Because the width of the beam must be narrow the width of the reflector must be several wavelengths wide, (Figure 7b) so antennas for the lower frequency radars become huge affairs. One BMEWS antenna is 165 feet high and 400 feet wide, and many antennas have dimensions of 50 feet or more.

On the other hand, radars called "height-finders" require a beam that is wide and short as in Figure 7c. An antenna to produce that beam must be tall and thin and often looks like a narrow portion of an orange peel (Figure 7d). Finally, certain radars called "tracking" radars need a thin "pencil beam" as in Figure 7e. This beam is usually produced by a circular parabolic antenna (Figure 7f).

There are three other parameters of a radar antenna that are of interest to an enemy—polarization, scan mode and location. *Polarization* refers to the orientation of the electromagnetic wave as it travels through space. Every electromagnetic wave consists of electric and magnetic fields which are mutually perpendicular and, by convention, polarization is the direction of the electric field. The receiving antenna must have an orientation to match the polarization of the incoming signal. In theory, if the incoming wave has perfect vertical polarization and the receiving antenna has horizontal polarization, *no* signal will be received. Such perfect isolation is never achieved in practice, but the fact remains that a vertically polarized antenna shows a great propensity for vertically polarized signals.

The scanning method used by the radar system refers to the motion of the antenna (or the beam) as the radar looks for targets.



A. VERTICAL FAN

C. HORIZONTAL FAN

E. PENCIL BEAM

B. SEARCH ANTENNA

D. HEIGHT-FINDER ANTENNA

F. TRACKING ANTENNA

FIGURE 7. ANTENNAS AND ANTENNA PATTERNS

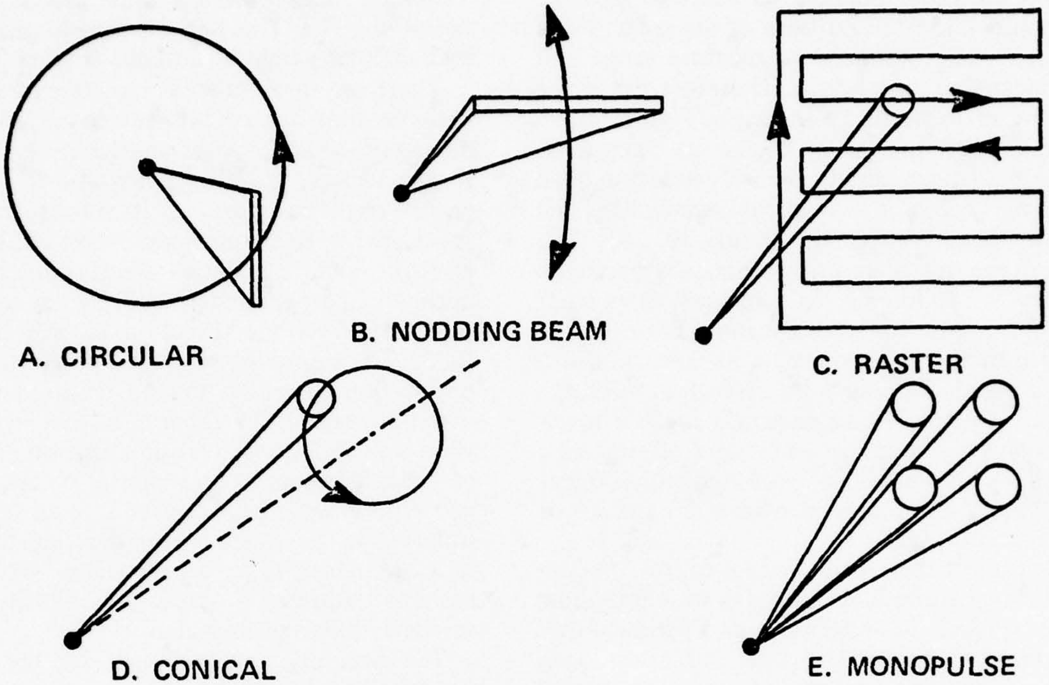


FIGURE 8. ANTENNA SCAN PATTERNS

We have already discussed the *circular scan* used by search radars (Figure 8a). They continuously rotate their vertical fan beam through 360° of azimuth at a constant rate, typically between 5 and 15 revolutions per minute. Other radars are not responsible for searching the entire volume of space around them. A height-finder radar, for example, is told, "There is a target at 047° and 80 miles. What is his altitude?" So the height finder operator rotates his antenna to an azimuth of 047° and then scans vertically from the ground up, a *nodding beam scan* (Figure 8b). The antenna pattern is a horizontal fan because the azimuth is known, the radar measures only elevation angle and range, and from those values calculates target altitude.

There are other instances where a radar need not search all of space. The fire control radar in the nose of an interceptor needs only to scan a volume straight ahead of the aircraft that is perhaps 10° by 10°. A method of doing this is the so-called *raster scan* because the pattern is similar to that used by a TV picture tube to "paint" the picture on the screen. The antenna has a pencil beam, not a fan, and it scans back and forth with a pattern of lines that cover the space (Figure 8c). There are several possible geometric patterns that are used for this procedure.

After one has acquired a target with whatever scan method was used, it is necessary for some types of radars to "lock-on" and "track" the target. This is equivalent to optically following the flight of an aircraft with a telescope. There are several ways this can be done. The two most common are *conical scan* and *monopulse*. With conical scan the pencil beam is nutated so that the center line of the beam describes a small cone in space with vertex at the antenna (Figure 8d). If the aircraft is on the axis of the cone, the strength of the target return remains constant. However, if the aircraft is not centered in the conical axis, the strength of the return varies in time as the beam progresses around the cone. The control circuits recognize which side of the cone is giving the stronger return, and a servo system repositions the antenna in the proper direction to keep the target centered. This same antenna pattern (a fairly wide pencil beam with a dimple in the center) can also be realized by sending out three or four slightly divergent pencil beams simultaneously. This technique is called *monopulse* (Figure 8c). If the strength of the return in one of the beams is stronger than in the others, the radar system knows that the target is off-center in the direction of that beam. Then the antenna is repositioned so that there is equal return from each beam. Thus the antenna follows, or "tracks", the target.

There is one final parameter of a radar set that is often overlooked because it is not an electrical parameter. That is the *location* of the radar set. The reason that we should consider this parameter seriously is that location is the one parameter of a ground radar that cannot be quickly changed. With varying degrees of difficulty, all minor, the operator can change the set's frequency, PRF, pulse width, polarization, scan mode, power and any other electrical parameter. Not so with his location. Thus one of the most common methods of characterizing a ground radar is its geographic location, and when this characteristic cannot be used, such as with a highly mobile radar, other electronic parameters must be used.

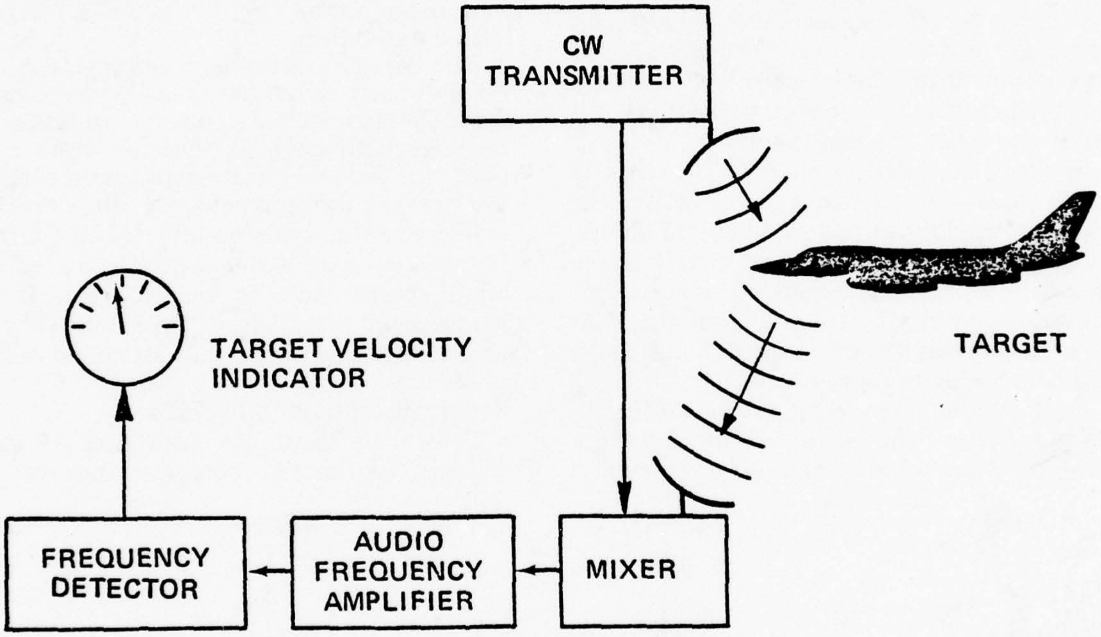


FIGURE 9. A DOPPLER RADAR

A Doppler Radar

You have seen the doppler principle and how slight the doppler shift is in a radar system compared to the radar frequency. How can such a slight frequency shift be detected? The shift will not be detectable by an ordinary pulse radar, especially one using a magnetron, because the transmitted frequency is not remembered during resting time. But in a CW radar it may easily be observed by mixing the transmitted frequency with the received frequency to produce a beat-frequency difference. Figure 9 shows a simple doppler radar. Since the transmitter is on continuously there is no duplexer and separate antennas are required for the receiver and transmitter.[8] Some of the transmitted signal is fed to the mixer to be mixed with the received signal. (Often leakage between the

[8] Radars with separate transmitting and receiving antennas are called *bistatic* radars.

transmitting and receiving antennas will be enough to provide the mixer with the transmitted signal.) The doppler shift will be the difference frequency produced by mixing the transmitted and received signals. Since the doppler shift (for ordinary target velocities and radar frequencies) falls within the audio frequency range, the signal from the mixer may be amplified by audio-frequency amplifiers. It is then applied to a frequency detector and a frequency meter to give a direct readout in target velocity.

The system outlined here is simple, but it has serious limitations. Since the transmitter is not pulsed the system cannot measure range and is severely limited in peak power capability. Separate transmitting and receiving antennas must be used to isolate the transmitter from the receiver and even so, leakage between the antennas can saturate the receiver and limit its sensitivity.

If we want the doppler radar to measure range, then we can frequency modulate the transmitter. However, as we discussed before, this procedure produces an ambiguity in the output because both target range and target radial motion produce frequency shifts. Thus this technique is not often used if both range and radial velocity are required.

A more common technique is the pulse-doppler radar. The major additions to the pulse radar are some capability for remembering the transmitted frequency and a signal processor to recover the doppler shift from the received radar echoes. The frequency memory is probably the most important of the two requirements because it affects the transmitter. With magnetrons one must lock an oscillator (called a COHO) to the transmitted pulse to preserve the frequency, and, this must be done after every pulse because the phase of the radar pulse cannot be controlled from pulse to pulse. Another technique uses master-oscillator power-amplifier (MOPA) transmitters in which the low-level oscillator runs continuously to provide the "memory" but the transmitter's power amplifiers are turned on for each pulse. One would typically find a klystron or similar microwave power amplifier as the last stage in such a transmitter.

The signal processing requirements for a pulse-doppler radar are basically the same as for a CW doppler radar, but the realization of there requirements can become quite complex. The particular form depends on whether the range measurement or the velocity measurement is more important. If the former is true then a delay-line canceller is used and blind speeds have to be accepted. If the requirement is the latter then filter banks are used and the radar typically has blind ranges.

Radar Susceptibility to ECM

Before we leave the discussion of radar systems, we should consider some of the

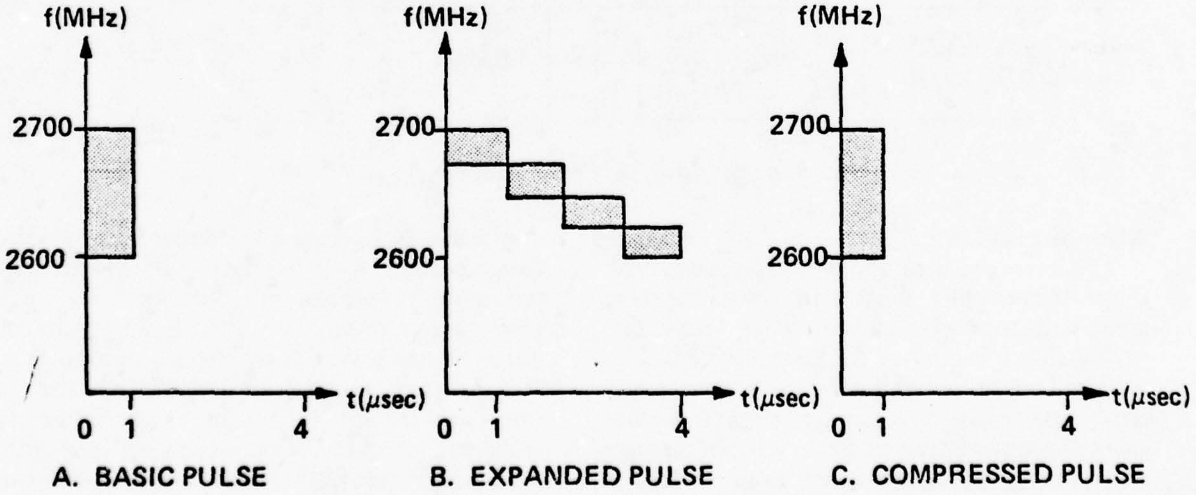


FIGURE 10. AN EXAMPLE OF THE PULSE COMPRESSION PROCESS

newer techniques that make a radar set more resistant to ECM. Many of these techniques involve changing some of the set's parameters according to some plan. PRF, frequency or pulse shape do not have to be constant, and special processing of the received pulse can convey some ECM immunity. Chapter 6 contains an extensive list of ECCM techniques but there are three that do warrant further discussion here because of their impact on radar system design.

Pulse Compression. The technique of pulse compression constituted a major advance in radar signal processing. Consider the conventional radar pulse. The peak power contained in the pulse is limited by arc-over in the tube or waveguide. Therefore, to get more energy in the pulse and increase detection capability, it is necessary to use a long duration pulse. Unfortunately range accuracy and range resolution are dependent upon a narrow pulse width at the receiver. Pulse compression allows us to resolve this impasse.

In order to visualize the process of pulse compression suppose we have a radar transmitter with a peak power capability of 1 megawatt transmitting a basic 1 μsec pulse with the time frequency diagram of Figure 10a. We want to expand the pulse to a 4 μsec length and at the same time cause the transmitted frequency to move downward from 2700 MHz to 2600 MHz as shown in Figure 10b. To do this we pass the basic pulse through the filtering and delaying network shown in Figure 11 prior to transmission. By delaying the lower frequencies more than the higher ones the pulse is dispersed over a longer period of time than the original pulse width. When the echo returns we send it through a compression network where the higher frequencies are delayed the most (Figure 12) and the various spectral components of the pulse are "stacked up" on top of one another, thus reassembling the basic pulse (Figure 10c). Notice that using this approach allows us to send out a megawatt, 4 μsec pulse with four times the energy of the basic pulse, yet we still retain the resolution capability of the basic 1 μsec pulse.

Normally we would not accomplish pulse compression using a set of band pass filters and delay lines. Instead we might use a *dispersive delay line* where the delay is a linear function of frequency. In the example

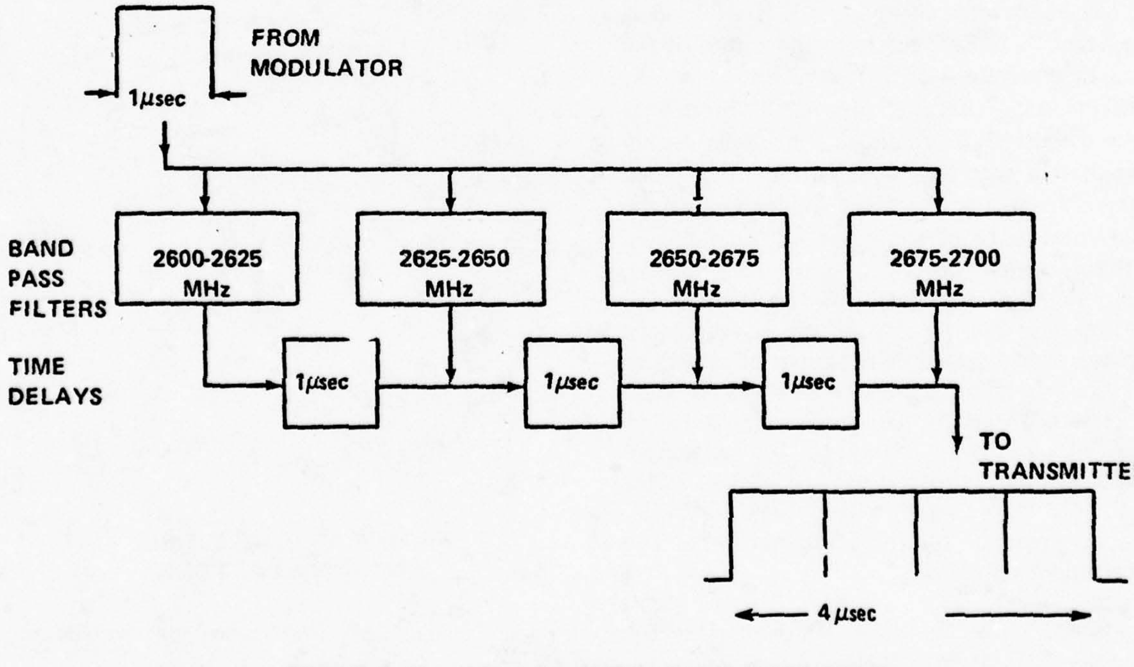


FIGURE 11. A PULSE EXPANSION NETWORK

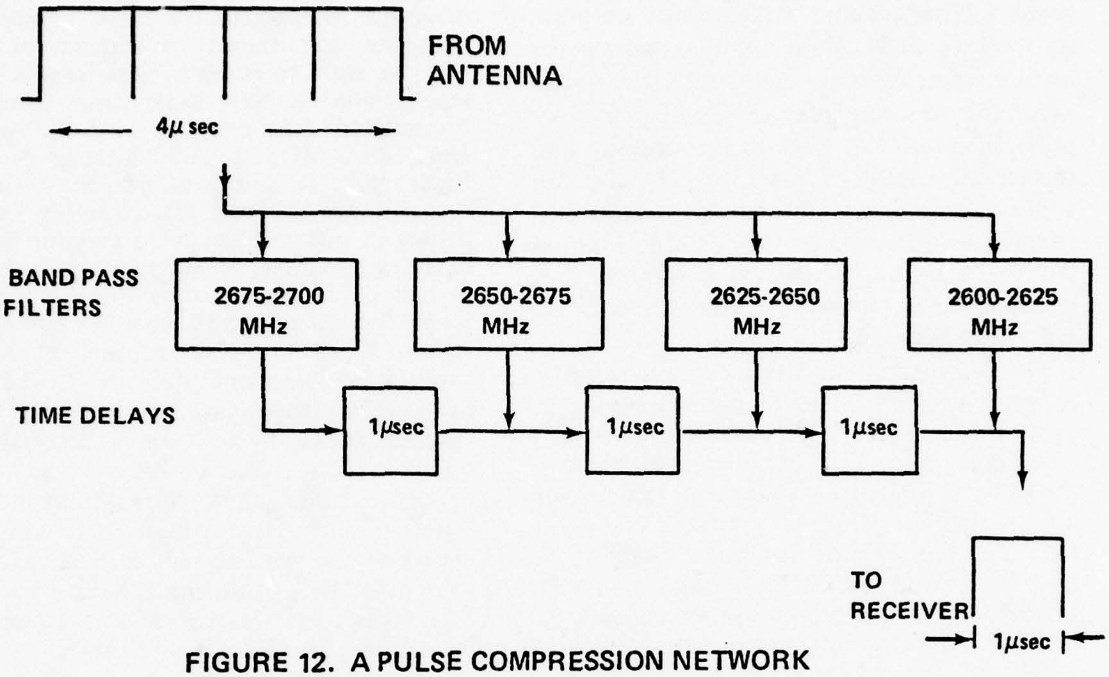


FIGURE 12. A PULSE COMPRESSION NETWORK

given the *compression ratio* is 4:1, in practice 10:1 is common and 100:1 seems possible.[9] Other names for this technique are "LIFMOP", an acronym for Linearly Frequency Modulated Pulse and "CHIRP" radar. The term "CHIRP" refers to the sound of the acoustic equivalent of this waveform.

Electronic Scanning. Up to this point we have discussed mechanically scanned antennas, that is antennas which derive their scan pattern from a mechanical movement of the total antenna or of some part of the antenna. This traditional method of scanning is simple, cheap and reliable, but it is limited in the rapidity and complexity of the scan pattern that can be produced. The advent of satellities and the growing complexity of tasks required of certain antennas has led to the development of electronic scanning. This extremely fast, scanning technique has a definite impact on the electronic warfare capability of a radar, thus its presence modifies the nature of the electronic threat.

To understand electronic scanning we need to understand how an antenna pattern is formed. Let us consider a short radiating element, that is, a length of wire short with

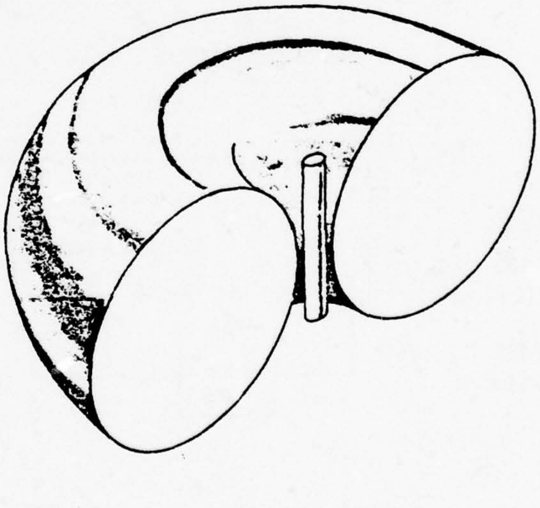
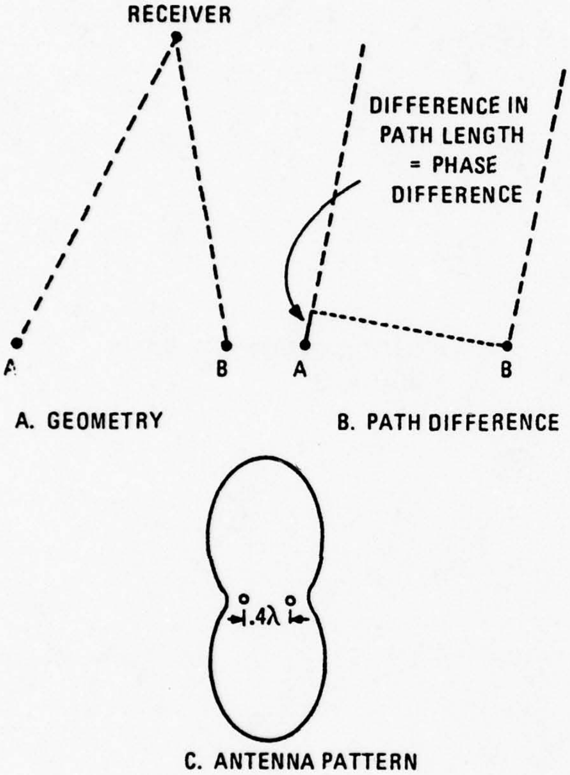


FIGURE 13. THE DIPOLE ANTENNA PATTERN

[9] H. O. Ramp and E. R. Wingrove, "Principles of Pulse Compression", *IRE Transactions on Military Electronics* (April 1961), 5:116.

respect to a spatial wave length of the energy radiated. Such a wire is called a *dipole* antenna. Electromagnetic energy is radiated from this element in a doughnut shaped pattern as shown in Figure 13. Now if we place a second element near this antenna (Figure 14a) and drive them both in electrical phase the amount of energy received at any distant point in space will be the sum of the energy received from each wire. Since electromagnetic energy travels at a constant velocity, the difference in distance from these two elements to the point of reception is equivalent to a phase difference (Figure 14b). Thus a point broadside to the two elements will receive maximum energy, a point off the end of the two element array minimum energy. The pattern for small spacing becomes that of Figure 14c where the phase difference is calculated by assuming that the reception point is so far distant that the rays from the two radiators to the reception point are essentially parallel. This pattern is commonly drawn as in Figure 14c, where the distance of the line from the center is proportional to the amount of energy radiated in that direction.



A. GEOMETRY

B. PATH DIFFERENCE

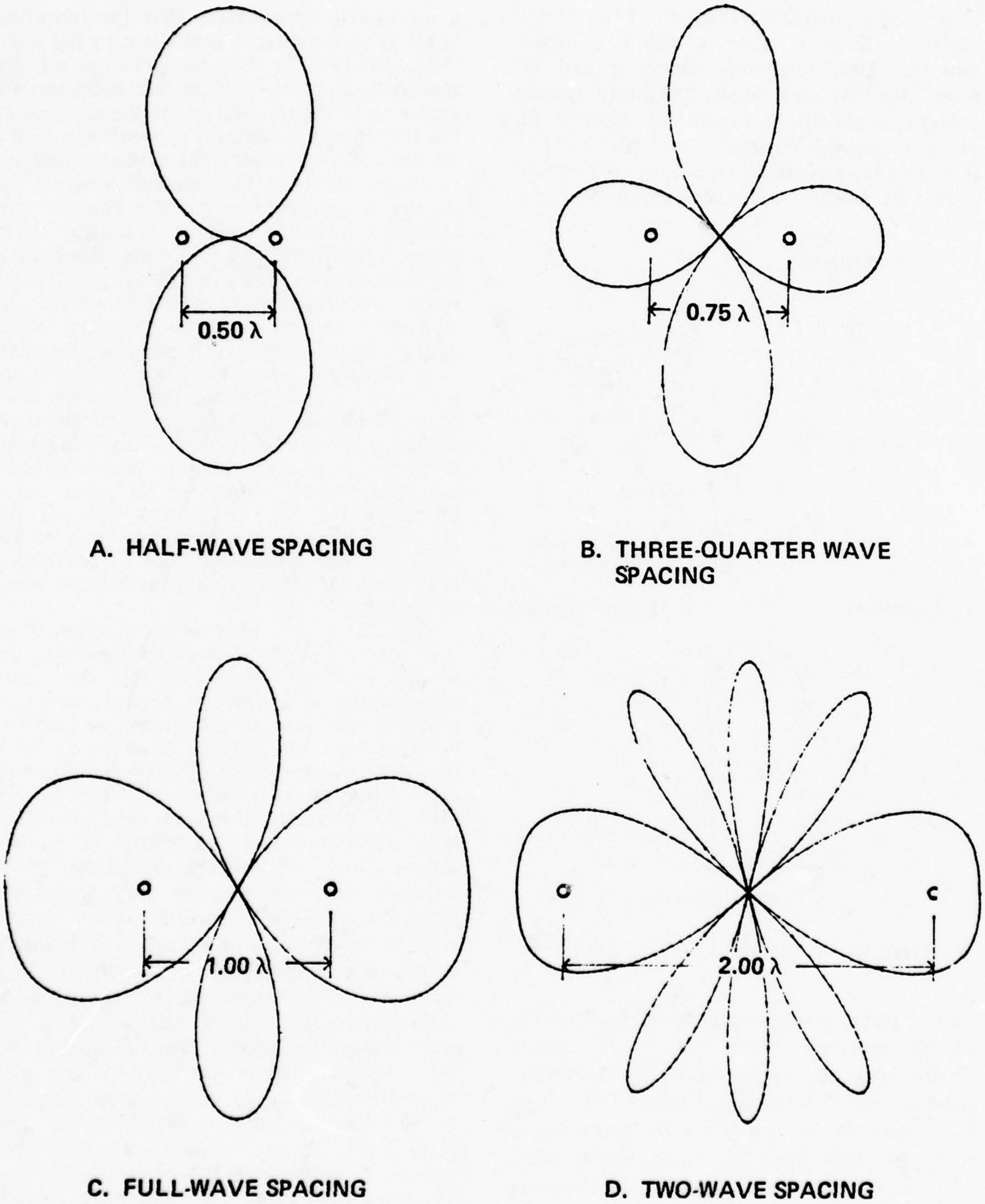
C. ANTENNA PATTERN

FIGURE 14. THE TWO-DIPOLE ARRAY

As we increase the spacing between the dipoles we will produce a null, a point of zero radiation, off the ends of the array as in Figure 15a. Continuing to increase the spacing between the two elements of this two-element array, or *interferometer* will create an additional pair of radiation lobes for every additional half-wavelength increase in separation. Of course, these interferometer lobes are not much help in determining direction since they are all equal, but adding other elements to the array all fed in phase (supplied with currents in phase with the end elements) accentuates the main lobe or main beam broadside to the array and reduces the sidelobes (Figure 16), although none of the sidelobes ever disappear. Thus by combining individual radiators in an array we can make an antenna.

Now let us ask what would happen if we vary the time phase between the elements, the dipoles, of an array. Under the same assumptions as before (a distant reception point so that rays to that point are parallel) we find that the pattern of an array with one-quarter wavelength spacing is symmetrically distorted (as in Figure 17). The pattern for a 90° phase shift between elements causes that configuration to be called an endfire array. Thus by varying the time phase between elements we can vary the space direction in which the antenna pattern points.

So if we construct an array of elementary antennas (in our illustration, dipoles) and vary the phase between elements we can move the main lobes of their combined pattern. If our array is one-dimensional, like the illustrations we have used, then the pattern has two symmetrical principle lobes, except possibly in the end-fire case. But if it is two dimensional as in Figure 18 then we can obtain a single steerable main lobe. The necessary phase control of these *phased arrays* can be achieved in two ways. One can change frequency creating a *frequency-scanned antenna*, or one can construct discrete phase shifters and control them with a computer.



A. HALF-WAVE SPACING

B. THREE-QUARTER WAVE SPACING

C. FULL-WAVE SPACING

D. TWO-WAVE SPACING

λ = WAVELENGTH

FIGURE 15. INTERFEROMETER ANTENNA PATTERNS

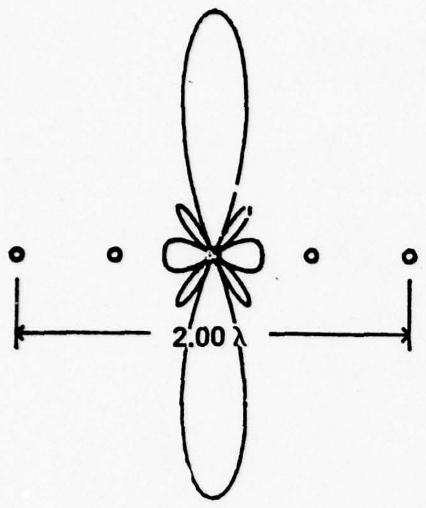


FIGURE 16. A BROADSIDE ARRAY ANTENNA PATTERN

Adding the computer not only allows us to move the beam very rapidly but we can also form a very complex scan pattern. In fact we can form any of the scans previously discussed (Figure 8) merely[10] by programming the computer. Furthermore, we can also reduce the sidelobes or form multiple main beams (for a monopulse radar, or for simultaneously looking at two objects) through the computer program. Thus, a phased array gives the radar tremendous flexibility in the antenna pattern.

Synthetic arrays. Since an antenna can be composed of many simple elements arranged in a line or one-dimensional array all being fed appropriately, it occurred to some people in the early 50s that one can also form a radar antenna array by moving a single element in a straight line and appropriately processing the result. Clearly, the processing involves recording the radar returns and then doing some sort of processing on the recorded result. The result is the synthetic array radar, so-called because the antenna pattern is synthesized from the results of a simple antenna moving in a straight line.

This type of antenna can be very attractive for airborne applications where the maximum antenna size is limited by the aircraft structure. Thus one can take an airplane with a 10-foot antenna and synthesize an antenna 1000 feet long. If this antenna is used to map the ground then the azimuth resolution of the radar changes from approximately 500 feet at 10 miles range to 5 feet at the same distance. The price that one pays for this resolution is, of course, the signal processing of the return.

It is shown in the literature on synthetic array radars that one simple processing scheme is to record the radar returns on film and then recover the map optically. The radar looks out to the side of the aircraft[11] (Figure 19a) and the radar returns are recorded crosswise on a slowly moving strip of film which is subsequently developed. A simple analysis shows that the film contains the scaled hologram of the ground when viewed by "light" of the radar frequency. If the developed film is illuminated by monochromatic light (say from a laser) then a real (radar) image of the ground will be formed and this image can be recorded on another film[12] (Figure 19c). Thus one can obtain high resolution radar maps of the ground from an aircraft.

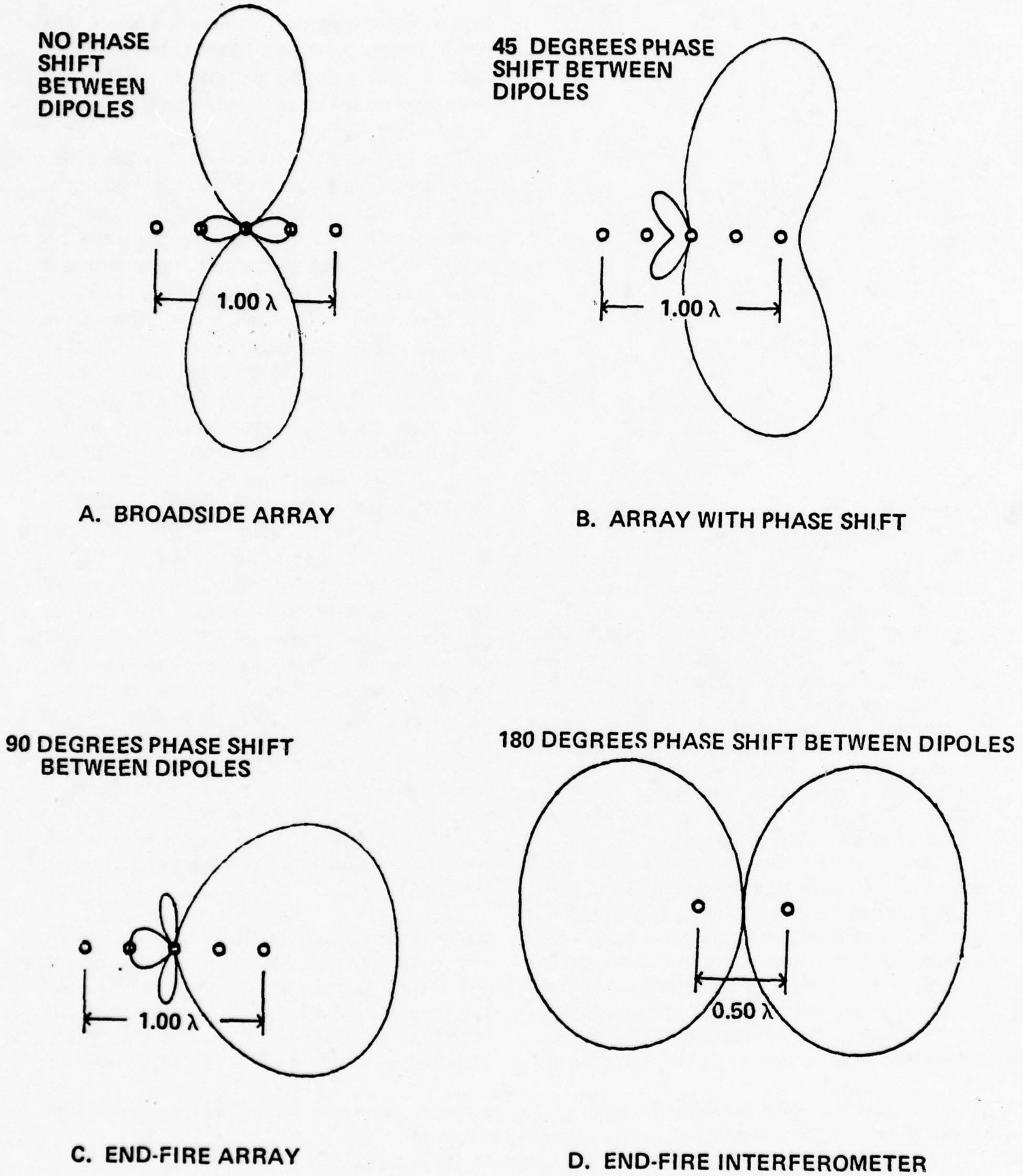
Radar Roles and Functions

Before we consider other aspects of the electronic threat let us summarize the employment of radar by listing the roles and functions of both airborne and ground radars. This list (Table 1) will not only show the

[10] Note that "merely" refers to the simplicity of the concept not the ease ot creating the computer program. One of the major costs in large phased arrays is the computer software.

[11] From whence the term "side-looking airborne radar"–SLAR–is derived.

[12] It is interesting that some of the early work on laser holography was a direct outgrowth of the work on synthetic array radars. The workers on the radar recognized that the laser was the optical equivalent of the single-frequency cw radar. See Robert O. Harger, *Synthetic Aperture Radar Systems, Theory and Design* (New York: Academic Press, 1970), pp 12–13.


NO PHASE SHIFT BETWEEN DIPOLES
1.00 λ
45 DEGREES PHASE SHIFT BETWEEN DIPOLES
1.00 λ
90 DEGREES PHASE SHIFT BETWEEN DIPOLES
1.00 λ
180 DEGREES PHASE SHIFT BETWEEN DIPOLES
0.50 λ

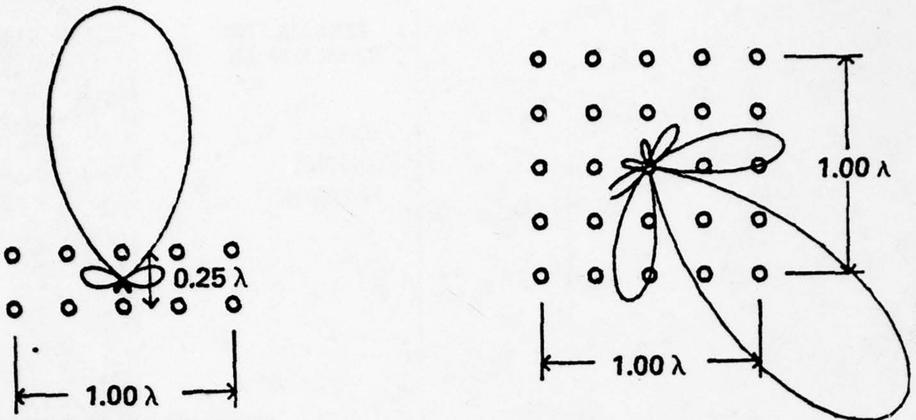
A. BROADSIDE ARRAY

B. ARRAY WITH PHASE SHIFT

C. END-FIRE ARRAY

D. END-FIRE INTERFEROMETER

FIGURE 17. ANTENNA ARRAYS WITH PHASE SHIFT



90 DEGREES PHASE SHIFT BETWEEN TOP AND BOTTOM ROW OF DIPOLES

PHASE SHIFT BETWEEN ADJACENT DIPOLES IS 90 DEGREES

A. BROADSIDE ARRAY WITH A REFLECTOR

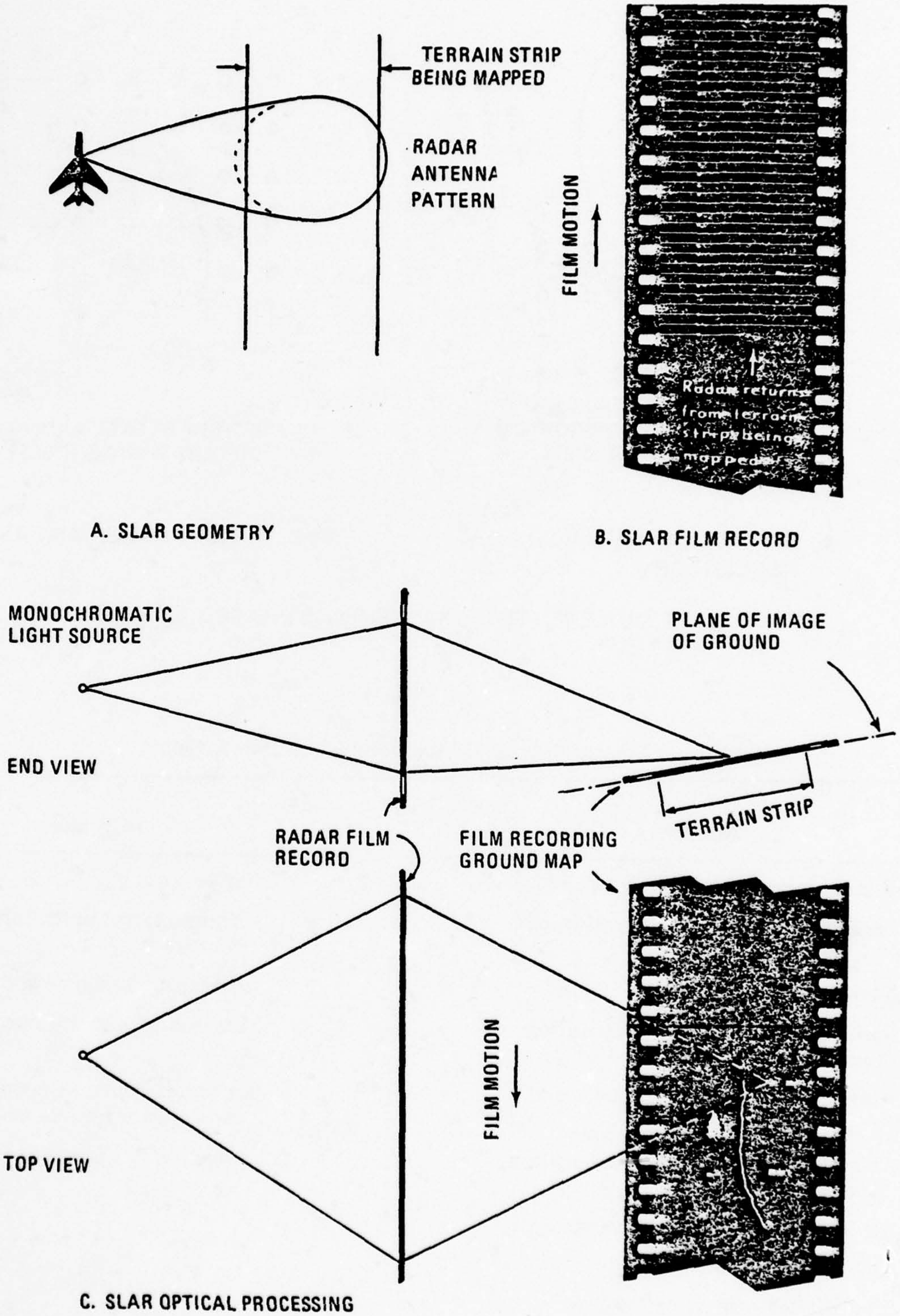
B. A 5 x 5 PHASED ARRAY

FIGURE 18. TWO-DIMENSIONAL PHASED ARRAYS

Table 1

Typical Roles and Functions of Air Force Radars

Airborne	Ground
Ground mapping	Early warning
Terrain following/Terrain avoidance	Airborne target detection, acquisition, tracking
Navigation	Interceptor guidance and control
Surface target detection, acquisition, tracking	Missile guidance and control
Air-to-ground weapon guidance and control	Air traffic control (navigation and collision/terrain avoidance)
Airborne target detection, acquisition, tracking	Identification friend or foe
Air-to-air weapon guidance and control	
Collision avoidance	
Identification friend or foe	



A. SLAR GEOMETRY

B. SLAR FILM RECORD

C. SLAR OPTICAL PROCESSING

TERRAIN STRIP BEING MAPPED
RADAR ANTENNA PATTERN
FILM MOTION
Radar returns from terrain strip being mapped
MONOCHROMATIC LIGHT SOURCE
PLANE OF IMAGE OF GROUND
END VIEW
TERRAIN STRIP
RADAR FILM RECORD
FILM RECORDING GROUND MAP
FILM MOTION
TOP VIEW

FIGURE 19. SIDE-LOOKING AIRBORNE RADAR

diverse use of radar in aerial warfare but it will also show the reason why much of electronic warfare concentrates on radar; it is one of the most pervasive electronic systems in the military force.

Other Radio Frequency Threat Systems

Even though the primary emphasis on electronic warfare tends to be concerned with radar threats, yet there are numerous other threats to military operations which must be considered. In fact, the impact of electronic warfare on these other systems may be greater than upon radar, if for no other reason than it is unexpected. For example, the initial use of electronic warfare by the British in World War II was against the German blind bombing systems, which were radio location systems, not radar. So we must spend a little time discussing these other threats. We will consider three groups of threats, passive detection including optical and infrared (IR) systems, radio navigation and location systems, and communications systems.

Passive Detection. A system which only receives energy (does not transmit energy) yet locates objects is a *passive detector system*. If an aircraft is navigating with an airborne radar, a receiver might detect the radar transmissions at a range much greater than the normal useful range of the radar. No range data would be available, but the azimuth would be known and triangulation using two reciever sites would give the aircraft position. Other passive detectors might operate acoustically or in the infrared range. These have shorter range but could be equally effective.

Another use of passive detection is for weapon terminal guidance[13] often called homing. Here some radiation from the target is used to direct the weapon to the target. For example, an infrared detection capability could be very helpful to an interceptor aircraft in the terminal phase of its attack. Since an object above 0°K radiates infrared energy due to the temperature of the body, an aircraft engine constitutes a major source of IR energy, especially an after burner plume. This plume (the hot exhaust gasses) is displaced from the aircraft, so it cannot be shielded, and allows detection attack from any angle. With passive guidance the victim may never know he is under attack until too late[14].

A third type of passive detection system is the optical system. You will recall that earlier in the chapter radar tracking of a target was described as being analogous to following the flight of an aircraft with a telescope . . . so why not use a telescope? Optical trackers are becoming more and more worrisome to the EW community. Optical tracking is not new, optics were coaxially mounted on some of our World War II fire control radars; and the operator could manually control the antenna to keep the reticule on the target if the radar failed. Now that there are several ways of jamming a tracking radar, many people are looking very seriously at optical tracking. The space program has proven with the Baker-Nunn cameras that optical tracking can be very useful. And the spectacular TV coverage of our moon shots has shown what optics coupled with TV can do. Furthermore, the development of night vision devices and low-light-level TV (LLLTV) cameras has given us the potential of extending our visual capability at night. Consider the importance of these developments in our context here. How do you jam an optical system?

Radio Navigation and Location. Traditionaly, radio navigation has encompassed low precision aids (accuracies on the order of miles) which are used to navigate aircraft to

[13] Weapon terminal guidance is usually classified as active (the weapon illuminates the target), semiactive (some other source illuminates the target, often the weapon launch system), and passive (guidance is by natural illumination or target generated radiation).

[14] Further comments on infrared and infrared countermeasures appear in Chapter 8.

the vicinity of the target so that more precise weapons guidance systems can be used. ADF, VOR, TACAN, and LORAN are examples of these systems. Although these systems are susceptible to electronic countermeasures, they have not received great emphasis because they are not used for weapons delivery. Rather their ECM susceptibility has been looked on as a means of harrassment, or of degrading or preventing operation in bad weather.

However, more recently radio location systems have been perfected to accuracies sufficient to permit weapon delivery. This idea is not new, the history in Chapter 1 contains several references to such systems; what is new is the improvement in technology allowing useful accuracies (accuracies of hundreds of feet or less). Thus it can be predicted that these systems will receive greater electronic warfare emphasis in the future.

The primary difference between the different radio location systems is the precise method used to measure location. Since these systems promise to become more important in the future, Table 2 lists the major types and their characteristics.

Communications. The various radio communications links that are scattered around the battle area must be considered as electronic threats. There are links from defense sites to their interceptors or missiles and back again, between all defensive and offensive military echelons, and between command posts and the offensive aircraft they control. How are these threats different from radar? First of all the transmitter and the receiver are at two different locations and the transmission path is one way, thus allowing for lower power levels than radar. Second, there is a much wider variety of modulation schemes available. There are AM, FM, pulse code modulation (PCM) and many others. Third, the bandwidth of a communication signal can be greater or less than radar. However, normally it would be less. Fourth, these signals could occur anywhere in the frequency spectrum, but they are more common at lower frequencies than radar. And fifth, the time of transmission is under control of the operator and less dependent on outside (enemy) influence. These five characteristics make communications electronic warfare more difficult and its success less widely publicized and discussed. In fact, the subject is so closely controlled that an overview is almost impossible to obtain, one is forced to discuss it in terms of electronic reconnaissance and communications security. Nevertheless many of the principles which are developed for radar electronic warfare apply (with suitable modifications) to communications electronic warfare.

Radio Frequency Spectrum Usage

Another characteristic of the threat is the frequency of each signal, or to state it another way, the portion of the frequency spectrum it occupies. A detailed listing of the frequency capability, the operating frequency and the operating schedule of each military emitter is very valuable information to an enemy. This information constitutes the electronic order of battle (EOB) and is carefully protected because of its military value. Furthermore such information is much too detailed for this text. Nevertheless it is possible to classify the typical operating frequencies of various military systems based on the characteristics of the electromagnetic radiation and the atmospheric transmission medium[15]. We have summarized this information for radio location systems in Table 3.

Similar information for communication systems is harder to specify because communications is not equipment oriented but system oriented. That is, a particular communications link between two parties may use a variety of equipments depending on the distance between parties, the amount of information to be transmitted, and the urgency of the information (priority). Table 4 classifies military communications into four catagories and give the characteristics of each.

Since higher frequencies have shorter range capabilities but wider bandwidth potential it is clear that the high volume administration and logistics traffic is preferentially sent by higher frequency links. The shorter ranges of these links, however, force the communica-

[15] See Appendix A for a discussion of radio wave propagation.

Table 2

Radio Location Systems

Technique	Intrinsic Accuracy[1]	Typical Systems[1,2]	LOP[3]	Number of Fixed Sites
Range–Azimuth	Variable	RADAR TACAN NAVARHO	Circle and radial line	1
Range–Range	Highest	DME SHORAN	Circle	2
Angle–Angle[4]	Least	RDF DF NAVAGLOBE ADF CONSOL VOR	Radial line	2
Differential[4] Range	Next Highest	LORAN OMEGA DECCA GEE DECTRA TOA (INVERSE LORAN)	Hyperbola	3
Differential Angle	—	—	Circle	3
Distance Sum	—	—	Ellipse	3

[1] Harry I. Davis, "Avionic Systems: An overview" (Course Notes, Course 867.12, Avionics Systems Engineering, UCLA, July 1972)

[2] Acronyms are defined in the glossary, Appendix F.

[3] Line of Position, the locus of points of constant measured value

[4] An angle-angle system is equivalent to a differential range system at great distances from the fixed site baseline.

Table 3

Spectrum Utilization of Typical Military Location Systems

Frequency Band[1]	System[2,3]	Range[4] (NM)	Accuracy (max.)
VLF	OMEGA	5000	1 mi
LF	GEE	—	—
	LORAN C/D	1200/500	.02–.1 mi
	DECCA	300	.1–1 mi
MF	ADF	300	2 deg
	STD LORAN	700	5 mi
HF	OTH Radar	1000	1 mi[5]
VHF	VOR	200	3 deg
	EW Radar	300	1000 ft[5]
	BMEWS	2000	1 mi[5]
UHF	TACAN	200	1 deg 1000 ft
	GCI Radar	150	500[5]
	SAM Radar	10-100	100 ft[5]
	AAA Radar	20	100 ft[5]
	IFF	300	—
SHF	Airborne Mapping Radar	100	50 ft[5]
	Airborne Intercept Radar	30	50 ft[5]
	AAA Radar	20	50 ft[5]
Infrared	Tail Warning	5	—
	FLIR	5	—
Optical	AAA Control	1-10	—
	LLTV	5	—

[1] Appendix F gives the frequencies of these bands under Frequency Band Designations.

[2] Systems used by both civil and military aircraft are included.

[3] Acronyms are defined in the Glossary, Appendix F.

[4] Typical maximum usable distance as limited by propagation or other factors.

[5] Estimated.

Table 4

Typical Military Communications Categories

Categories	Priority	Usage	Distance
Strategic Command and Control	Highest	Low	Long
Tactical Command and Control	Next Highest	Low	Short
Operational	Moderate	Moderate	Short
Administration and Logistics	Lowest	High	All

tions system to be quite extensive if the distances covered are long. Since short range systems are relatively more secure, then all the other categories of traffic will use the administrative system unless some other factor prevents this, such as the mobility of one party. Thus the particular frequency usage of any particular military force will depend both on their particular requirements and the sophistication of their communications system.

Signal Density. All of the various threats we have discussed are fairly well understood, and sometimes easily countered. However, when there are many different types of threats existing simultaneously, it severely taxes the capability of an already busy pilot or EW operator. And, of course, when an airborne penetrator gets closer to his target the problem increases because the defense is more dense near a valuable target.

In a normal, overlapping-coverage air-defense situation one could expect to have the maximum radar spacings given in Table 5. From this table one can see that a penetrator might have to be concerned with several dozen threats simultaneously. Furthermore as the penetrator moves through the battle area, he is continually being confronted with new threats. The reason for making this point about the density of signals in a defended area is to insure that we don't get so restricted in our perspective that we fail to appreciate the extreme difficulty of operating in a high-signal-density environment. An example of the signal densities which can be expected in combat is the report that there are over 100 SAM batteries on the Egyptian side of the Suez Canal[16]. Since each SAM battery transmits several signals this could easily equate to 300–500 signals in that area.

To this density of air defense signals one must add the communications and radio location signals required by the penetrator. If the air battle is taking place over the battlefield then one must also add the ground (or naval) electronic signals. The result is to make electronic warfare operations a very complex task requiring well designed equipment and tactics to cope with the high signal densities encountered.

Table 5

Typical Radar Spacing

Radar Type	Maximum Useful Range	Maximum Spacing
Early Warning	230 nm	150 nm
GCI	140 nm	100 nm
Long Range SAM		
Acquisition	140 nm	50 nm
Track	80 nm	
Short Range SAM		
Acquisition	115 nm	15 nm
Track	20 nm	
AAA		
Acquisition	25 nm	5 nm
Track	10 nm	

[16] Miller, "Soviet Radar Expertise," p 14.

Chapter 3

BASIC CONCEPTS OF THE ELECTROMAGNETIC CONFLICT

Introduction

Historically, Electronic Warfare developed as a series of electronic counters (ECM) to specific electronic systems. This approach was valid as long as the electronic systems were few and noninteracting. However, today a modern air defense system can employ a large number of radars integrated through a command and control communications net. To propose ECM without considering the total system is both to attack the problem piecemeal and to risk never defeating the defense. Because a preponderance of electronic warfare is concerned with penetrating enemy air defense systems we will preface our discussion of the basic concepts of electronic warfare with a brief discussion of air defense systems. A more detailed discussion of air defense will be found in Appendix C.

There are basically two types of air defense systems a penetrator or group of penetrators must cope with: area defense systems and point (or terminal) defense systems. These two systems are invariably connected to a third system, the warning system, whose function it is to alert the other two systems. Table 6 summarizes these three systems.

A point defense system exists in close proximity to a valuable resource, such as a major industrial site, a strategic military installation, or a densely populated urban area. The defenses immediately surrounding Washington DC, Moscow, or a major command and control center such as Offutt AFB, and the Safeguard system defending ballistic missile launch sites are examples of point defenses. A point defense consists of Anti-Aircraft Artillery (AAA)[1] and Surface-

Table 6

The Three Basic Types of Air Defense Systems

Defense		Sensors	
System	Weapon	Ground Based	Weapon Based
Warning	Area/Point Defense	Early Warning Radar	—
Area	Interceptor	Ground-Controlled-Intercept Radar	Radar Infrared Optical
	Long Range SAM	Acquisition or Tracking Radar	Radar Infrared
Point	Medium/Short Range SAM	Acquisition or Tracking Radar Optical	Radar Infrared
	AAA	Radar Optical	Radar

[1] This terminology is not the same as the US Army terminology primarily because we have very few guns in our air defense system. See Appendix C for a more detailed discussion.

to-Air Missile (SAM) batteries which serve the purpose of directly attacking penetrators in the near vicinity of the defended target.

The area defense system serves three purposes: (1) to turn back the attack by forcing an unacceptably high fuel or payload penalty on penetrators avoiding the defense, (2) to force attrition upon the penetrators before they reach the point defense boundaries (which makes the point defense problem somewhat easier) and (3) to prevent wanton destruction of marginally important areas. Its weapons must have a much greater range than the point defense weapons; currently the interceptor and the long range SAM are used.

The function of the warning system is to alert the defense to the presence (or the imminent arrival) of the penetrators, to give the defense gross positional information on the penetrating force, and to determine the size of the attacking force. This warning allows the more complex area and point defense systems to come to a state of full readiness so that their response time is minimal.

ECM can be targeted against the sensors of all three systems. But against the warning system any radiation intended to degrade the operation of the sensor has the unfortunate effect of alerting the defense that a threat exists; hence the warning system is fundamentally different from the other two systems. Therefore, the most effective tactic is often to do nothing to disturb the defense until the penetrators are sure that the warning of their arrival has been passed. Thus ECM against the warning system often takes the form of radio and radar silence–the complete cessation of all electronic emmissions–until it is almost certain that the penetrators have been detected. Nevertheless one does not want to wait so long that the defense has determined the track and size of the penetrating force. Another effective tactic is the *feint* or false penetration to distract the attention of the defense from the real attack and to create uncertainty as to the size and direction of attack. Once the defense is warned then ECM can revert to its more conventional role of degrading the defense radars.

Since ECM has negative utility against the warning system in general, the warning system will be ignored in much of the discussion that follows. This lack of emphasis is not to be interpreted as a reduction in importance of the warning system but rather an attempt to avoid confusion by discussing opposing tendencies simultaneously. It must be always appreciated that adequate warning can result in a five- to ten-fold reduction in the defense response time to the penetrators.

Intelligence, ESM, and RHAW

When operating against an integrated defense network it is essential that the penetrating force have information about the location and technical characteristics of the electronic systems ranged against it. Traditionally, this information has been called reconnaissance or electronic reconnaissance (ER). Recently this term has fallen into disfavor because its long association with intelligence has obscured the fact that reconnaissance has a broader meaning. The collection of information about the enemy electronic systems really falls into three distinct classes determined by who controls the collection and the use of the information. The classes are called intelligence (ELINT, COMINT, SIGINT, etc.), Electronic Warfare Support Measures (ESM), and Radar Homing and Warning (RHAW).

The foundation of the whole subject of electronic warfare rests upon a well-developed knowledge of the enemy electronic systems. This is the proper function of intelligence. It requires a long term effort and it culminates in the specification of the capabilities of the enemy weapon systems (Scientific and Technical Intelligence), the disposition of the enemy weapons (specifically the Electronic Order of Battle), and the strategy the enemy will use in the employment of his weapons (his battle tactics). This information is necessary to develop effective weapons and tactics, and to target our weapons to obtain our objectives. Thus intelligence, or the lack of it, forms the backdrop for the combat that is electronic warfare.

When the tactical commander comes to the point of planning tomorrow's mission, however, he needs more than this extensive background information; he also needs to know the precise state of the enemy's electronic defenses. It is not enough to know that there are so many AAA sites and SAM sites in the defense, he wants to know precisely where they are located, whether any have moved since the previous day, and if any new ones have appeared. He is also vitally interested in their tactics, e.g. if they have tried new approaches to defense. The value of the information to him is directly proportional to its currency. Hence, he has a legitimate need to request that certain reconnaissance be performed to satisfy his immediate needs. This reconnaissance is ESM because it will be quickly processed in response to the tactical commander's needs. The sources of ESM may be diverse; it may come from a regularly scheduled collection mission, or it may come from the debriefing of aircrews returning from the previous mission. In any case it will be subject to a minimum of formal analysis because of time constraints.

After the aircrews have launched on their mission they are in need of further information about the defense. For the defense commander has the option of responding to the penetration as he thinks best, so the penetrators must not count on a fixed response. To respond to a SAM defense with tactics appropriate for AAA defense could produce an unpleasant surprise. Thus the aircrew wants to know the type and location of the defense weapon engaging him.

But the aircrew member is busy, he does not have time to adjust a precise, sensitive intercept reciever used by the intelligence collector or ESM collector to determine the threat to his aircraft. He wants the equipment to be automatic, to examine the received signals and flash him the appropriate warning. Therefore any signal analysis capability of RHAW equipment must be based upon an extensive background of intelligence painstakingly collected, so that its response in the tactical environment can be immediate.

Table 7

The Three Types of Electronic Reconnaissance

Type	Intelligence (ELINT)	ESM	RHAW
Operational Control	Intelligence collection agency	Tactical commander	Aircrew
Collection time	Greater than 24 hours before takeoff	Between takeoff and 24 hours before takeoff[1]	After takeoff
Analysis	Extensive	Minimal	Pre-planned or Built-in
Use	Equipment & Weapon Development Electronic Order-of-Battle Targeting	Mission Planning	Aircrew Protection

[1] This is an estimate based on conversations with combat aircrews.

The distinctions between these three classes of reconnaissance on the basis of operational control are summarized in Table 7. Even though the table makes the distinctions appear clear cut, these distinctions are not accepted by all.[2] For all three classes require the same objective acts: the collection of information about the enemy electronic system. And sometimes one collector (RHAW) can provide information for all three classes of reconnaissance. These conceptual distinctions are also affected by organizational conflicts, which invariably occur when the same data is used for two different purposes by different persons with different but overlapping responsibilities. Hence the relationship of these vital parts of electronic warfare to the whole is partly pragmatic and partly theoretical. Consequently we may expect further changes in definitions.

The ECM-ECCM Ladder

Having understood that electronic warfare is an interaction between friendly and hostile electronic systems, we may well ask what is the nature of this interaction? How does Electronic Warfare interact with electronic systems to reduce their effectiveness or deny their use to the enemy? One traditional way of expressing this is to say that ECM resembles a ladder. That is, an electronic system results in a countering electronic system—ECM; the ECM in turn causes a counter-countermeasure—ECCM—to be implemented; and this process continues *ad infinitum*. One can diagram this process as shown in Figure 20.

This analysis shows that we can never achieve unequivocal superiority through ECM. Unfortunately this analysis tends to promote a two-valued evaluation of ECM: ECM either works or it doesn't, depending on what rung of the ladder we are on. However, a more realistic evaluation of this chain yields the following conclusions:

1. The real effectiveness of ECM lies somewhere on a spectrum ranging from completely effective to completely ineffective. The actual value of this multivalued evaluation depends both on the position of the conflict on the ladder and on many other factors, some relating to training and morale and others relating to the uncertainties of combat.

2. ECM techniques normally have only a finite time of superiority. Eventually the enemy will develop a counter technique and the superiority would pass to him. Thus one cannot expect a certain ECM technique to give indefinite superiority.

3. As a result of the previous principle, the real advantage of ECM is that it gives relative superiority while the enemy is developing and deploying the countermeasure. This relative advantage can be measured by the time delay between the operational employment of two successive steps on the ladder. This time delay can be reduced by advance information on electronic systems under development, hence good security is necessary to preserve the relative advantage.

4. A corollary to the previous principle is that electronic warfare is very reactive and

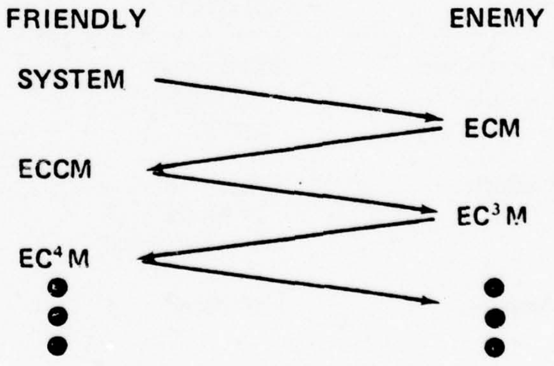


FIGURE 20. THE ECM LADDER

[2] It is argued by some, and not without merit, that the distinction between ESM and intelligence is a false issue. In their view the intelligence organization can and must provide timely information to meet the commander's needs. Furthermore, they say that it is immaterial how he obtains the information he wants about the enemy, and professional resources can do a better job than resources under his control. Such theory is indisputable but realizing it may be another matter. Practically speaking, any organization responds to the person who has fiscal control, so that control of ESM by the tactical commander may be a practical necessity.

time urgent. That is, if an enemy develops an effective system then we are under considerable pressure to develop the countermeasure quickly and cut down his advantage. Hence, rapidity of development is often an electronic warfare requirement. This is reflected in the existence of QRC (quick reaction capability) procedures which omit some of the normal avionics development steps in an attempt to speed up the development process for electronic warfare equipment.

5. Another real value of ECM is technological superiority, the ace-in-the-hole idea. However, this concept cannot be extended indefinitely unless a continuing program of development is pursued, because the enemy may anticipate our development and out-distance us if our technology remains static. Furthermore this concept concentrates on the surprise attendant on the initial use of ECM. Consequently it has much more application to peace-time development of ECM than to wartime.

6. Finally, *we should not fail to develop a technique because it has a simple counter. For we benefit from the inevitable delay between the time that the enemy is certain that we are using the technique and the time that he can make the counter operational. In that time we can be working on (anticipating) the next step in the ladder to maintain our technological superiority.*

Although the ECM ladder provides a useful concept of electronic warfare it does not really help one evaluate the effectiveness of ECM in combat for several reasons. First, as we noted before it fosters a two-valued measure of effectiveness. Second, it tends to concentrate on the interaction of only two electronic systems rather than consider the complexity of combat where many systems are employed simultaneously. Third, it tends to exclude the human operator. And forth it ignores the great difference between peacetime and wartime ECM development. Before we consider the human operator let us place ECM into the overall context of combat.

ECM and Conflict Management

It appears that one primary motivating factor of a military force in combat is the *exchange ratio*. The exchange ratio is defined as the ratio of the enemy resources destroyed or captured to the friendly resources expended. A commander plans his tactics to achieve both a favorable short-term exchange ratio and a favorable long-term exchange ratio. It is his exchange ratio goal which determines both his emphasis on training and morale and his requests for additional and/or new equipment. The diagram of Figure 21 attempts to show how the exchange ratio influences the development and procurement of crew members, and avionics and weapon systems, where avionics is broken out separately even though it may be a component of weapon systems.

From Figure 21 you will note that the exchange ratio and the commander's desired exchange ratio are combined to form his perceived combat situation. Another input to the combat situation is called "goals". This additional input models the fact that there may be other influences which override the exchange ratio. For example, in a tactical ground battle the goal of a favorable air exchange ratio may be overridden if the FEBA (forward edge of the battle area) is retreating.

The Wartime Structure. The important concept in Figure 21, however, is not the interconnections between the separate elements *per se*, but the structure resulting from the interconnections—closed loops of interconnections. It is a fundamental concept of feedback control theory that this "closed-loop" structure can produce a wide variety of dynamic behavior of greater complexity than the behavior of the individual elements themselves,[3] especially if the elements are non-linear. This concept has been applied to industrial and urban organizations by Forrester and other Industrial or Systems Dynamicists, and they have shown that this "causal" loop structure can produce most of

[3] See any good text on feedback control theory. The older texts, of which the following is one, may be easier to understand because the mathematics is less sophisticated: J-C Gille, M.J. Pelegrin and P. Decaulne, *Feedback Control Systems: Analysis, Synthesis, and Design* (New York: McGraw-Hill Book Company, Inc, 1959). Incidentally, on page 15 this book uses a military organization as an example of a feedback

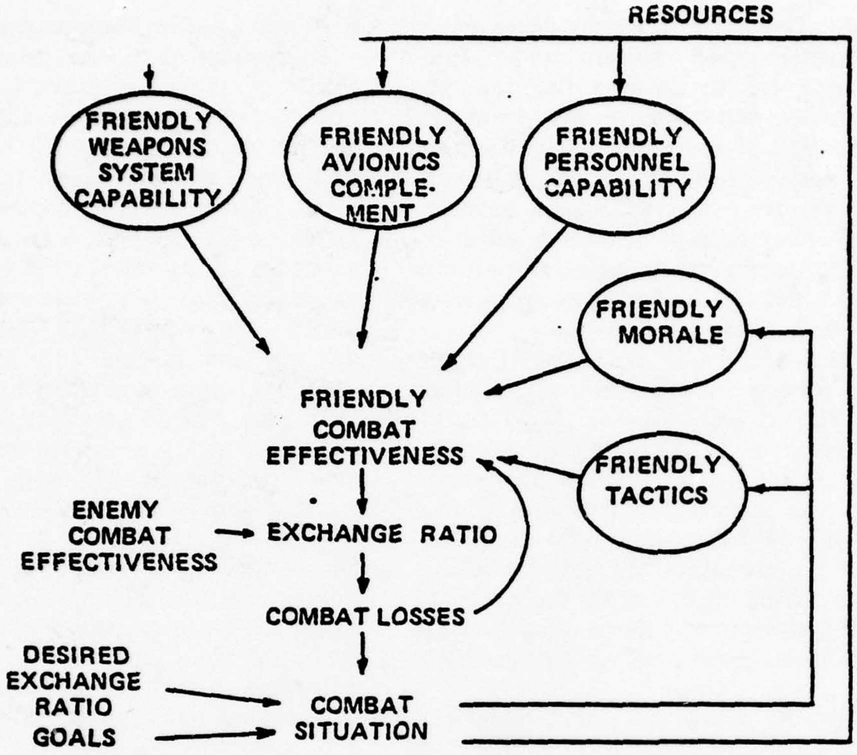

RESOURCES
FRIENDLY WEAPONS SYSTEM CAPABILITY
FRIENDLY AVIONICS COMPLE-MENT
FRIENDLY PERSONNEL CAPABILITY
FRIENDLY MORALE
FRIENDLY COMBAT EFFECTIVENESS
FRIENDLY TACTICS
ENEMY COMBAT EFFECTIVENESS
EXCHANGE RATIO
COMBAT LOSSES
DESIRED EXCHANGE RATIO
GOALS
COMBAT SITUATION

FIGURE 21. THE FRIENDLY MILITARY SYSTEM

the characteristic behavior of industrial and urban organizations.[4] Thus this structure appears useful for discussing the influence of electronic warfare on the battle.

The idea that we wish to use is that feedback loops tend to either oppose the original stimulus or to reinforce it. The ormer are called "negative" feedback loops n feedback control theory, the latter positive". Negative feedback tends to produce goal-seeking behavior; however, the aracteristics of the elements themselves pecially time delays) can change a smooth l-seeking behavior into wildly oscillatory avior. Positive feedback tends to produce exponential growth.[5] The interaction between these two behaviors when coupled by non-linear elements can give a complex dynamic behavior whose character changes with time depending upon the situation. [6,7]

Now if we consider the three outer loops of Figure 21, which contain the commanders material resources, we discover they are all negative feedback loops.[8] Thus they can produce a wide variety of dynamic behavior. Furthermore, their major components have widely different time delays—that is, they respond at different rates to a demand by the commander for more and better resources. For example, the personnel loop (crew

[4] Jay W. Forrester, *Industrial Dynamics* (Cambridge, Mass: MIT Press, 1961).

[5] Jay W. Forrester, *Principles of Systems* (Cambridge, Mass: Wright-Allen Press, Inc, 1968), Chapter 2.

Forrester, *Industrial Dynamics*, p 200.

One fascinating aspect of this analysis is that it provides an objective view of something we have emotional, ential knowledge of—human organizations. Often our involvement in organizations prevents us from ively analyzing them.

hese six loops and their delays are discussed in more detail in Appendix E.

training and replacement) has a delay varying between a few weeks and a year. The avionics loop has a development and procurement delay ranging between 6 months and 3 or 4 years, while the weapons system loop has a development and procurement delay varying between 1 and 10 years.

On the other hand, the three inner loops, combat losses, morale and tactics all have delays in the order of months and, most important, have the potential of being positive feedback loops depending on the battle situation. In addition, from a mathematical viewpoint, all the loops are non-linear especially the inner loops, thus they can dominate the system unexpectedly. The resulting potential for exponential growth (or decline) in the exchange ratio clearly implies the potential for victory or defeat if these loops dominate the system.

From the above discussion it is clear that changing the outcome of the battle through training, avionics and weapon development is a slow process. Hence, the tactical commander tends to use tactics—Surprise, Mass, etc.—to achieve a favorable daily exchange ratio and relies on the other three loops to maintain a desirable long-term exchange ratio. ECM, containing elements of the tactics, personnel and avionics loops has the potential to influence the conflict in both the short term and the long term, depending upon the mix of elements used. If the ECM avionics is available and personnel are trained then ECM tactics can procure definite short term advantages. On the other hand, long term advantage can only be obtained through continuing avionics development since the enemy will react to nullify a tactical ECM advantage as the ECM-ECCM ladder shows.

The Peacetime Structure. One of the real problems of ECM in peacetime is that this causal flow diagram changes, for the simple reason that there is not a daily confrontation of the two forces. Instead, we must rely on intelligence to estimate the exchange ratio (Figure 22). In so doing we invariably forecast enemy capability because intelligence has both a long time delay (in some cases more than 10 years) and a great difficulty in producing accurate estimates of the enemy tactics. But forecasting tends to overestimate the enemy capability both because we do not want to be surprised and because it is built on a poor data base.[9] Furthermore, it is reasonably clear that forecasting in industrial organizations tends to accentuate undesirable behavior,[10] and there seems to be a similar effect here—often called the "10-foot tall" enemy. Hence, in peacetime, development is often characterized by very long delays and insufficient intelligence.

It should be clear now that the ace-in-the-*hole concept of ECM applies best to a* peacetime ECM development because it has the potential for a very favorable exchange ratio at the onset of hostilities. But after the initial confrontation has occurred the enemy will adjust his forces to obtain a better exchange ratio, hence a continuing development must be maintained to preserve this advantage.

This brief discussion has attempted to put ECM in its total context. We have seen some of the advantages of ECM as a medium-response-time tool for swinging the battle in our favor. We have also seen some of the reasons for the difficulty of ECM development in peacetime. From this evaluation the idea of a wide-ranging ECM development program to preserve the options of the combat commander (i.e. give him the ability to respond quickly to an undesirable exchange ratio) becomes very reasonable.

Now let us return to a more microscopic view of electronic warfare. We want to consider a view of electronic warfare which will incorporate the human operator and the diverse systems and diverse modes of operation which characterize combat, and which leads to a multivalued evaluation.

[9] Any military power of necessity conceals as much of his present industrical development capability as possible. See also Edward B. Roberts, "Exploratory and Narrative Technological Forecasting: A Critical Appraisal", *Technological Forecasting*, 1, No 2 (Fall 1969): pp 113-127.

[10] Forrester, *Industrial Dynamics*, pp 437-444.

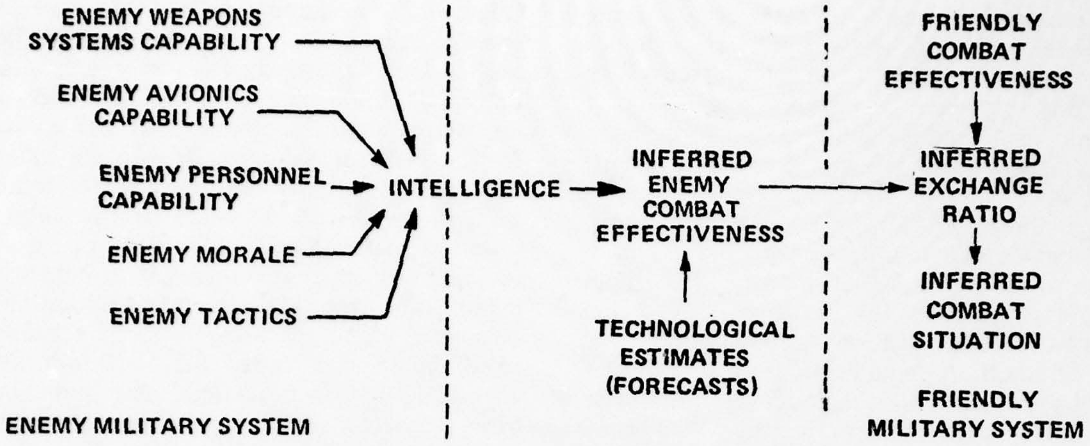

ENEMY WEAPONS SYSTEMS CAPABILITY
ENEMY AVIONICS CAPABILITY
ENEMY PERSONNEL CAPABILITY
ENEMY MORALE
ENEMY TACTICS
INTELLIGENCE
INFERRED ENEMY COMBAT EFFECTIVENESS
TECHNOLOGICAL ESTIMATES (FORECASTS)
FRIENDLY COMBAT EFFECTIVENESS
INFERRED EXCHANGE RATIO
INFERRED COMBAT SITUATION
ENEMY MILITARY SYSTEM
FRIENDLY MILITARY SYSTEM

FIGURE 22. THE PEACETIME COMPETITIVE VARIABLE

ECM and Systems Operation

In an actual combat engagement an electronic system can have many different modes of operation whose use will depend on the quality of its input signal. In an environment devoid of hostile electromagnetic emanations, the system is normally operated in an *automatic mode*. The effectiveness of this mode is often very sensitive to the quality of the input data. If the input data is "clean", i.e., free of enemy ECM, the system has excellent capability; but increasing ECM intensity can cause the system to lose effectiveness swiftly (Figure 23). When the situation becomes unbearable the operator will switch to some *manual mode* of operation which typically has less capability in a "clean" environment, but has some capability when the automatic system has failed catastrophically.

The manual mode is also subject to degradation by ECM although it usually degrades more slowly than the automatic mode.[11] This slow degradation is a result of the tremendous adaptability of the human operator. Although human response times are constrained by a lower limit, and the brain can be saturated by excess data, a trained operator is skilled in discarding extraneous data and will rapidly learn to cope with new situations. In essence the man changes his algorithms as the situation demands, something automatic equipment cannot do.

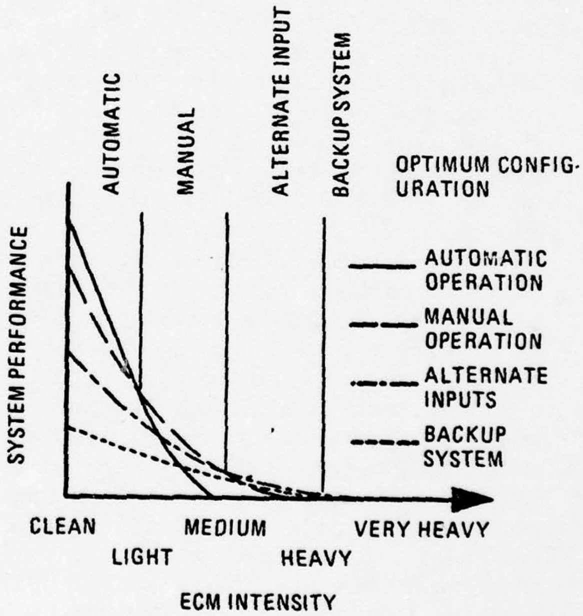


FIGURE 23. SYSTEM DEGRADATION WITH ECM

[11] The idea that human operators are more ECM resistant than automatic systems is almost an axiom in electronic warfare. As far as is known it has never been proven, and it may be that no general proof is possible.

As the ECM intensity increases the input data to the manual system will become more and more unusable or unreliable, and an operator, no matter how proficient, is ultimately limited by input data quality. Eventually the operator will attempt to get data from other electronic sensors, that is, from *alternate* inputs. Again, these data sources are subject to degradation but they are (presumably) less sensitive to degradation then the primary sensor operating in the manual mode or less likely to be attacked by ECM because of infrequent use or some other reason. Therefore, it is possible that there would come a point at which no reliable electronic data is available to the operator, in which case it would be necessary for him to rely on less desirable *backup* systems (optical, sonic, etc.) which are not seriously affected by ECM.

If all these options are available, then a system has four modes of operation in the face of ECM:

Automatic Mode
Manual Mode
Alternate Input Mode
Backup Mode

It is reasonable to expect that the relative performance of the four modes in the face of ECM will be shown in Figure 23. In that case the system will obtain the best effectiveness in the face of increasing ECM by switching to successively less capable but more ECM-resistant modes.

Since ECCM is generally the counter to ECM, this sequence of modes of system operation is also an outline of a method of ECCM design to give maximum performance in the face of ECM. Thus this concept of avoiding a catastrophic failure by "gracefully" falling back to other modes of operation can be called the *ECM/ECCM interaction.*

If all the system modes are not available to the operator, he will not have the maximum possible ECCM capability. For example, if no manual mode were available, the presence of sufficient ECM intensity could lead to complete failure of the automatic mode. Then the operator would be forced to use the alternate input mode which would give him less capability than he would have if he could operate in a manual mode. As a result the use of ECM could lead to a substantial advantage. A corollary of this concept is that the *most vulnerable system is the completely automatic system which has no manual mode*, because if the system fails, there is no other option.

This concept can also be applied to the major subsystems of each defense weapon system (See Appendix C for a description of these major subsystems). When this is done one has the potential for evaluating the performance reduction of any weapon system due to ECM.

In this concept we have not specified how the ECM intensity is produced. In general, the measurement of ECM intensity is very difficult in a combat situation. For the total ECM intensity may be the combined result of several diverse systems operating at separated geographical locations. The picture is further complicated by the fact that several nonelectronic techniques tend to be considered as ECM.[12] Thus quantifying the abcissa of Figure 11 is very difficult.

ECM and Tactics

All equipment used to enable a force to penetrate a hostile defense is usually described by the single term *penetration aids* or *penaids.* This term includes such items as ECM equipment and RHAW equipment. The great majority of penaids are directed against radars because these sensors are the eyes of the defense and are therefore accessible, while other electronic equipment, such as communications, is geometrically inaccessible. To understand the radar-penaid interaction we need to understand both the employment of ECM and the types of ECM. We shall look first at the general situations concerning ECM and then at specific ECM types.

The Four Tactical Situations. There are four commonly accepted ECM situations which have tactical implications and these are listed in Table 8. The *one-on-one* situation is the traditional design point for ECM situations and it represents the defense-penetrator

[12] See Chapter 5 for a more detailed discussion of ECM.

Table 8

ECM Tactical Situations

		Number of Penetrators	
		one	more than one
Number of Defense Systems	one	one-on-one (1:1)	many-on-one (N:1)
	more than one	one-on-many (1:N)	many-on-many (N:N)

duel when the defense weapon is engaging the penetrator, i.e. the duel is in its terminal stage. At this point the penetrator is isolated and identified. The desirability of this tactical situation to the penetrator depends on the effectiveness of the penetrator's ECM and the options available to both penetrator and defense. If the penetrator's ECM is effective and precludes any other options (for example, if the penetrator ECM will prevent AI radar tracking and the weather is IFR[13]) then the situation is desirable. However, the localization of the penetrator makes the possibility of other defense options high.

The *many-on-one* situation is a penetrator attempt to prevent the duel from entering its terminal stage. In some cases this situation is called *mutual support*. The objective is to overwhelm the defense so that it cannot effectively single out a single penetrator for one-on-one duel. On the other hand, the defense is likely to react by attempting a *one-on-many* situation in which the penetrator is overwhelmed by many threats. The result of these two tendencies is that the combat situation becomes *many-on-many*. Consequently penaids must be effective in both the one-on-one situation and the many-on-many situation.

Since the one-on-one situation usually represents the terminal stage of the defense-penetrator duel, penetrator survival in the face of this terminal defense usually assumes priority over other mission items at that point. If ECM is unable to guarantee survival unaided, the penetrator will have to employ some sort of maneuver. Thus the probability is high that the penetrator's mission effectiveness will be degraded, even if the penetrator is not destroyed. (For example, defensive maneuvers in the bomb run could result in greatly increased CEPs). Thus the defense stands to benefit by forcing the duel to the one-on-one, or better yet, the one-on-many situation. Conversely the penetrator stands to benefit if the situation is never allowed to progress to that stage.

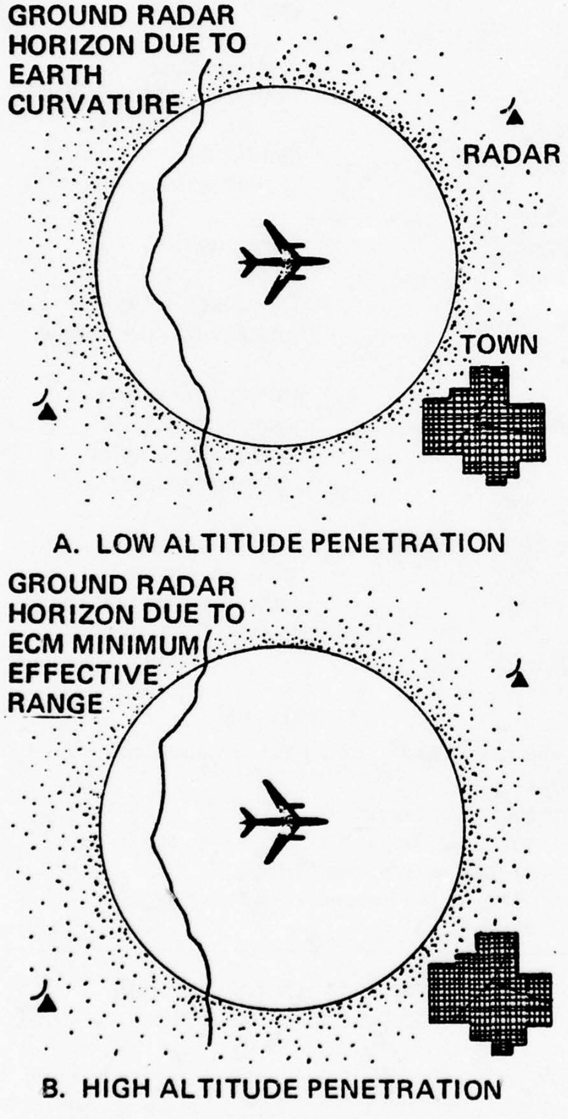
The previous analysis impacts on the phrase "search radars never killed anyone" which is often used as justification for concentration on ECM against typical one-on-one threats. The phrase is obviously true, however the permitting of the defense surveillance net to operate undegraded is tantamount to giving it the option of forcing the conflict to the one-on-one or one-on-many situation at will, i.e., the penetrator runs the guantlet unaided.

In this context it is clear that one of the advantages of low-altitude penetration is to force the defense away from the one-on-many to the one-on-one situation. In addition, the reaction time available to the defense is greatly reduced. It appears that the advantages gained by low-altitude penetration are worth the cost in range-payload, navigation accuracy, etc. If we insist on high-altitude penetration we must replace the geometric advantage of earth curvature with some

[13] Instrument Flight Rules, implying flight in Instrument Meterological Conditions (IMC)—without visual contact with the ground or with a true horizon.

penaid or tactic if we are to maintain the survivability of the force. The most logical candidates are speed and ECM, both of which are required for good surviability.

Speed of itself, as Appendix C shows, primarily compresses the defense reaction time, but high altitude places the attack under surveillance for a greater distance, thus negating most of the advantage of speed. But ECM is most effective at long ranges (see discussion of burnthrough in Chapter 5), and at high altitudes ECM has access to a large number of radars. Thus high altitude ECM has potentially a great impact on the defense; its effect is to make the aircraft clearly visible only at medium to short ranges. This, in effect, restores the radar horizon limitation lost by going to high altitude (Figure 24), and now the speed advantage of high altitude can directly compound the defense problem by reducing their reaction time. The result potentially could be more potent than low altitude penetration by itself. Hence, high-altitude penetration must rely on ECM against the search and acquisition radar net.


GROUND RADAR HORIZON DUE TO EARTH CURVATURE
RADAR
TOWN
GROUND RADAR HORIZON DUE TO ECM MINIMUM EFFECTIVE RANGE

A. LOW ALTITUDE PENETRATION

B. HIGH ALTITUDE PENETRATION

FIGURE 24. LOW AND HIGH ALTITUDE PENETRATION HORIZONS

The Two Classes of ECM. The tactical situation not only affects our dependence on ECM but it also affects ECM itself. To understand these effects we must understand the general characteristics of ECM.

As noted in Chapter 1 there are two general classes of radar ECM: Jamming and Deception. The general characteristics of each class are given in Table 9. This tabulation reveals that in general jammers have a simpler data processing requirement, a simpler signal requirement, and conceal the aircraft at the expense of requiring more power. Deception, on the other hand, has a smaller power requirement per radar countered at the expense of more stringent signal waveform and data processing requirements. In addition, deception makes no attempt to conceal the aircraft, rather it seeks to distract the attention of the defense system through false or misleading information.

Although the entries in the table will be discussed in more detail in Chapter 5 it is felt that they are generally self-explanatory except for the problem areas (Item #7). For jamming it can be shown that against most radars the aircraft is concealed beyond a *minimum effective range*. Hence, this range becomes an important limitation of the ECM. In addition, the jammer must periodically check the radar frequency to determine if the radar is on the same frequency. If the jammer signal is continuous (often the case) then the jammer must be turned off periodically so a receiver can *look-through* the jamming to observe the radar signal. And the *frequency*

Table 9

The Two Basic Types of Radar ECM

1.	Generic Name	Jamming	Deception
2.	Equipment Types	spot jammer barrage jammer sweep jammer	false target generator repeater gate-stealer track breaker
3.	Primary Effect	deny position and velocity[1]	produce false position and velocity
4.	Signal Type	dissimilar to radar echo	similar to radar echo
5.	Data Processing Required by Jammer	frequency set on[2]	false position false velocity frequency set on[2] number of false targets
6.	Power Required by Jammer	proportional to radar peak power	proportional to number of false targets and radar average power[3]
7.	Primary Problems	minimum effective range[4] frequency coverage look-through passive detection	credible motion credible target echo-broadening passive detection

NOTE: This Table considers only the effects of ECM on the sensor itself, not on the command and control system.

[1] Velocity refers to radial velocity derived from doppler frequency measurements.

[2] The requirement that the jammer frequency be the same as the radar frequency.

[3] A major advantage of deception is that it requires less power than jamming (see Chapter 5).

[4] Also called burn-through range or self-screening range. This is the primary reason for the large power requirement of jamming.

coverage of the continuous signal must be great enough to jam all radars in line-of-sight even if they have different frequencies. Finally, both types of ECM can be detected by enemy receivers independent of the radars themselves. Hence, the ECM reveals itself to *passive detection*.

In addition to passive detection, the major problems of deception are producing a *credible target* with *credible motion*. For a false target to be credible its return must have an apparent doppler shift if it has radial motion. In addition, the deceiver ideally should produce a long term consistent motion that makes the false target seem to be realistically moving (credible motion). The problem of *echo-broadening* is really that of trying to make the ECM echo look like a true radar echo. Because of antenna pattern effects it is not uncommon for the false target to be much wider than a normal echo, so that the system can easily distinguish between the true and the false.

Tactical Situations and ECM. The two types of ECM of Table 9 respond differently to the tactical situations of Table 8. For the penetrators, the major effects are felt in the power and data processing requirements and these relate directly to the size and complexity of the ECM. Hence, these determine the cost of ECM. For the defense the major effect is also felt in the data processing rate and power requirements, and these in turn determine the cost of the defense.

However, there is another factor that enters the picture to determine ECM effectiveness: the effect of the problem areas for each ECM type. Depending upon the situation, this factor can either enhance or degrade the penetration effectiveness. This factor will also be included in the comparisons.

Table 10 compares the two types of ECM and the no ECM case ("clean") in the one-on-one, one-on-many and many-on-one situations. The comparison is made assuming a fixed power per defense radar (P). The data rate requirement comparison is made on a per penetrator and per defense radar basis, assuming that each defense radar causes a specified data rate at each penetrator (R_p) and likewise each penetrator causes a specified data rate at each defense radar (R_d).

Table 10

ECM and the Tactical Situation

ECM	Clean			Jamming			Deception		
Tactical Situation	1:1	1:N	N:1	1:1	1:N	N:1	1:N	1:N	N:1
Defense Power per Penetrator[1]	P	NP	P	P	NP	P	P	NP	P
Penetrator power per defense radar[1,2,6]	--	--	--	P_p	$P_p - P_p/N$	NP_p	FP	FP/N	NFP
Penetrator data rate[3]	==	==	--	R_p	$NR_p - R_p$	R_p	R_p	$\geqslant NR_p$	R_p
Defense radar data rate[4,5,6]	R_d	R_d	NR_d	$\geqslant R_d$	$\geqslant R_d$	$\geqslant R_d$	FR_d	FR_d/N	NFR_d

NOTE: This table assumes all radars and penetrators can "see" each other. R_p and R_d are defined in text.

[1] P = average power, P_p = peak power = average power ÷ duty cycle.

[2] The smaller value for 1:N jamming assumes frequency diversity (see Chapter 6); The larger, no frequency diversity.

[3] The smaller value for 1:N jamming assumes no frequency diversity, the larger, complete frequency diversity.

[4] One basic effect of ECM is to input false data into the radar so that the defense radar data rate per radar can only increase in the face of ECM. The data rate of the defense command and control network may increase or decrease under ECM conditions depending upon its response to the increased radar data rate.

[5] The data rate increase due to jamming is difficult to determine because of the dissimilarity between the jamming and the radar signal.

[6] F = the number of false targets. It is assumed that the F false targets are divided among all the defense radars.

Examing this table shows why ECM effects can be so variable; we have eight different quantities, all interrelated, even when we have simplified the problem by ignoring all other factors. If we look more closely we see that numerical advantage generally increases both the power and data rate seen by the opponent. Since the relative power determines the concealment range, both power and data rate are important. A more detailed examination, however, shows that the two types of ECM behave differently. Jamming is inherently less affected by defense numerical superiority than is deception. This is especially true if the defense radars are close together in frequency, since one jammer can easily cover all of them. In essence the jammer must only determine if a radar is unjammed. However, this advantage is paid for by the greater power requirement of the jammer.

On the other hand the deceiver is greatly affected by defense numerical superiority, especially if the deception is to be practiced against all radars simultaneously. For in this case it must correctly associate all the received radar pulses with the correct radars so it can uniquely match its transmissions to their pulses. If the radars are close to each other in frequency then the sorting problem (called the "de-interleaving" problem) is not simple and requires considerable data processing.

A Numerical Example. A numerical example may make these effects clearer. Let us assume all defense radars have the parameters listed.

Average radar echo power at penetrator:	1 watt
Pulse width:	1 μ sec
PRF:	100 pps

These parameters have been chosen to make the numerical calculations easy, not to simulate any particular radar. Note that we will make our comparison at the penetrator since the propagation path back to the defense radar is the same for both radar echo and ECM. Thus the power battle is decided at the penetrator.

From those three parameters the following parameters can be derived:

Radar duty cycle:	.01%
Peak radar echo power at penetrator:	10 Kw
Radar echo spectral power density:	1 w/MHZ

In addition, we will assume that the ECM is effective when its strength equals that of the radar echo (0dB S/J ratio).

Now let us look at the jamming case. For the one-on-one situation, the jammer has to generate 10 Kw average power. If the single penetrator is facing 10 radars all on the same frequency (no frequency diversity) then 10 Kw is still adequate since each radar can only use its own radar echoes. If these 10 radars are all on significantly different frequencies then the required power increases to 100 Kw. Likewise the penetrator data rate increases as the number of significantly different radar frequencies increase; but the defense data rate per radar, although more than clean case, stays constant since there is only one penetrator. However, the defense does have to triangulate to find the penetrator so the command and control data rate does increase. On the other hand, if there are 10 penetrators and one radar then the total ECM power becomes 10 times that of a single penetrator so that the radar data rate increases while the penetrator data rate remains the same.

In the deceiver case let us assume that the objective is to place 10 false targets into the defense system. Since the deceiver requires 1 watt at .01 percent duty cycle for every false target generated, 10 watts of radiated ECM power are needed with the penetrator accounting for every radar pulse. If a single penetrator faces 10 defense radars, then his 10 watts will still produce 10 false targets, but unless he puts appropriate false targets on each radar the defense can eliminate these false targets by comparisons between radars, at the cost of an increase in defense system data rate. Meanwhile the penetrator has to keep track of the pulses from 10 different radars. If the radars are on 10 significantly different frequencies, the penetrator data rate increases 10-fold; if the radars are on the same frequency then the penetrator data rate probably increases 100-fold, since he must sort (de-interleave) the pulses.

If we have 10 penetrators against one radar and still require 10 false targets per penetrator then each penetrator still requires 10 watts, at a reasonable data rate. But now the defense sees 100 false targets, with a consequent 100-fold increase in data rate.

Table 11

The Effect of Defense Numerical Superiority on the ECM Problem Areas

Problem	Cause	Effect
Minimum Effective Range	Defense Radar more likely close to Penetrator	Defense has more time to observe penetrator
Lookthrough	Penetrator more likely under observation by more than one radar	Penetrator less able to determine threat
Frequency Coverage	Greater Frequency Diversity	Less penetrator ECM power against each defense radar
Credible Motion	More radars to be countered	Greater penetrator data processing capability required
Credible Target	More radars to be countered	Greater penetrator data processing capability required
Pulse Broadening	More radars to be countered on a pulse-by-pulse basis	Greater penetrator data processing capability required
Passive Detection	False intersections	Pure triangulation by defense becomes more difficult

The ECM problem areas all become more serious as the defense gains the numerical ascendancy, except passive detection.[14] Table 11 gives the causes and the effects. The effect on passive detection is often misunderstood, and is commonly called the "deghosting" problem.[15] Possibly the misunderstanding arises because active radar returns are very effective in eliminating the ghosts.[16]

The question of who has the ascendancy in the many-on-many situation is hard to resolve since it is a function of both the relative numbers of penetrators and defense radars and of data rate saturation. On the one hand, the defense does have one disadvantage which can be exploited: its radars are relatively immobile compared to the penetrators. Thus they cannot rapidly increase the number of radars in the penetration area to force the penetrators into a numerical disadvantage, consequently the penetrators can choose the area of engagement if they are not constrained by their target selection. On the other hand, by the use of mobile radars which can be set up in a matter of hours, the defense can capitalize on the ESM delay of the

[14] Using the radar purely in a listening mode.

[15] It is easy to underestimate the computational difficulty of determining which of the multiple intersections represent aircraft. Chapter 5 contains a more detailed discussion of this problem.

[16] A false intersection is called a "ghost".

offense and present the penetrators with unexpected defense concentrations.[17] Thus the outcome of the ECM battle is extremely difficult to predict.

Deception. Before we leave our discussion of ECM and tactics we need to say a little more about deception. It should be clear that attacking a defense system with deception requires both considerable computation, much more than for jamming, and confidence in the ECM for the exposed aircraft return is concealed by electronic "slight of hand". Since the penetrator is payload limited, this required computation is very costly, especially if we are not supremely confident of our technique. Yet in the 1:1 situation, the power advantage of deception over jamming is hard to ignore, and the data processing requirement is modest if the single radar has a strong enough signal to make it easy to identify. Thus deception has a definite place in protecting single penetrators from terminal threats, where the situation is almost always 1:1.

Table 12

An ECM Scenario

Defense System	Attack Force
3 EW radars	1 stand-off jammer
2 GCI radars	2 waves of four attack aircraft equipped with on-board ECM
1 SAM acquisition radar	
1 SAM tracking radar	
3 AAA tracking radars	
Numerous non-radar controlled AAA	

Since there are some missions which invariably involve single penetrators, for example, photoreconnaissance, there is high payoff in having some effective (uncompromised) deceivers available for use. This in turn creates a demand for detailed technical intelligence since deception, by its very nature of requiring a signal similar to the victim radar signal, requires detailed information about the enemy radars. This in turn leads to a sort of "black market" in

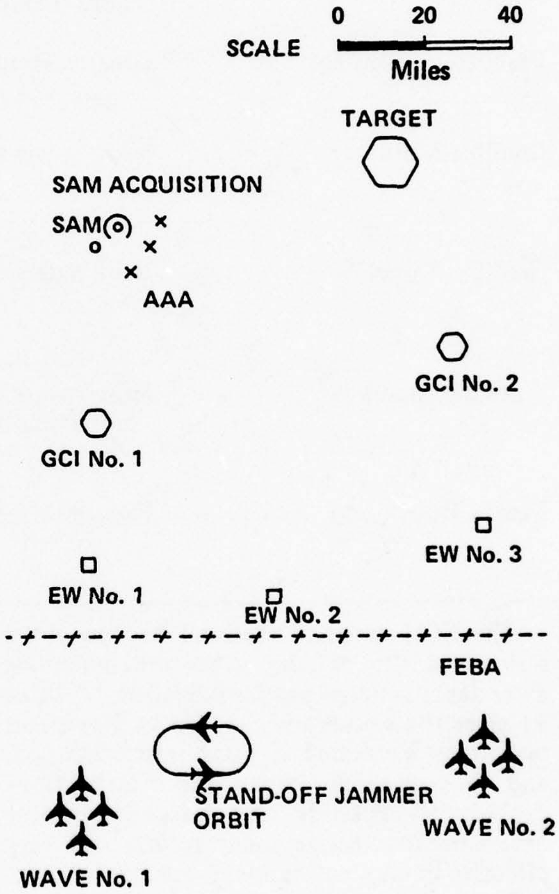


FIGURE 25. A TACTICAL AIR DEFENSE MODEL

[17] In a netted defense, mobile radars are not without complications. Unless the site has been used previously, a new site must be "harmonized" with the rest of the system; that is, its position and orientation with the rest of the system must be established so that aircraft seen by it can be correlated with aircraft seen by the remainder of the system. Otherwise, raids could be grossly overestimated.

weapons-systems and to commando type exploits such as the British (and Israeli) raids mentioned in Chapter 1. This nature of deception means that it is also very susceptible to compromise, since the enemy, by slight equipment modifications, may change the radar characteristics enough to negate the deception.

An Example of Tactics and ECM

The analysis of the many-on-many situation is further complicated by tactics, that is deployment of aircraft to achieve numerical or electronic superiority at particular points in the mission profile. Thus every situation must be considered separately. The combined effect, however, is to force the conflict to the favorable many-on-one situation. The defense, on the other hand, will attempt to use its forces to gain the upper hand also, so tactics must be responsive to changes in the defense.

As an illustration of the effect of tactics in enhancing the effect of ECM consider the following model of a defense system under tactical air attack (Table 12).

For simplicity, the defense system is assumed to be completely netted in support of the SAM and AAA which protects some target area, Figure 25. We will examine the events as they might take place in time.

Stand-Off Jamming. A stand-off jamming aircraft typically has independently operating jammers. For the purposes of illustration let us postulate it has ten jammers. And, each jammer functions independently in some frequency range, say E-Band.[18] The aircraft jams a victim radar by feeding noise power into it through both the main beam and the side lobes.[19] The immediate result of side-lobe jamming is to deny target acquisition (or more literally to cloud-up the scope presentation of the victim radar) beyond some given range. For the purpose of this analysis, let us assume that we wish to deny acquisition of attacking aircraft outside some range, say 20 miles.[20] To accomplish this task, we might use our standard-off jammer resources as follows:

1 Jammer on EW #1
1 Jammer on EW #2
2 Jammers on EW #3
2 Jammers on GCI #1
2 Jammers on GCI #2
2 Jammers on SAM Acquisition Radar

As a rule of thumb, if we propose to jam through the side lobes we should realize that the lower the side-lobe level of the victim radar the more difficult it is to jam. Typically EW antennas have large side-lobe levels so they are relatively easy to jam. EW #3, on the other hand, because it is further away, requires two jammers to make up for loss of power due to distance. This same comment holds for the SAM acquisition radar. Correspondingly, the GCI with a smaller side-lobe level requires two jammers each. Although it is certainly desirable to jam the SAM tracking and missile launch radar through the side lobes, the SAM side lobes are sufficiently suppressed that practically the entire resources of a stand-off jammer would have to be devoted to one SAM. This same argument is true for the AAA tracking radars.

Using the above simplifications, we may now draw circles of radius 20 miles around each victim radar (Figure 26) keeping in mind the assumptions made and the refinements required. It is clear that our ECM has greatly

[18] See Appendix A.

[19] Radar antennas are generally directional which means that most of the power is directed out in front and only a small portion spills over to the sides or back. In addition. radar antennas have the same receiving pattern as transmitting pattern. Thus, it is simple to force noise power into a radar system through the main beam but rather difficult, although possible, to introduce it by illuminating the side or back (side lobes) of the victim radar. For example, to introduce equivalent amounts of noise power into a radar receiver, it is reasonable to require that 1,000-10,000 watts be forced into the side lobes for each watt injected into the main beam.

[20] It should be clear that, although burn-through radius is a useful concept, it is subject to refinement with appropriate probability distributions. For example, radar scintillation may make some aircraft visible to an experienced radar operator even in the presence of jamming. Additionally, the radar cross-section measured in equivalent square meters changes dramatically with various aircraft aspects (as much as 1000:1).

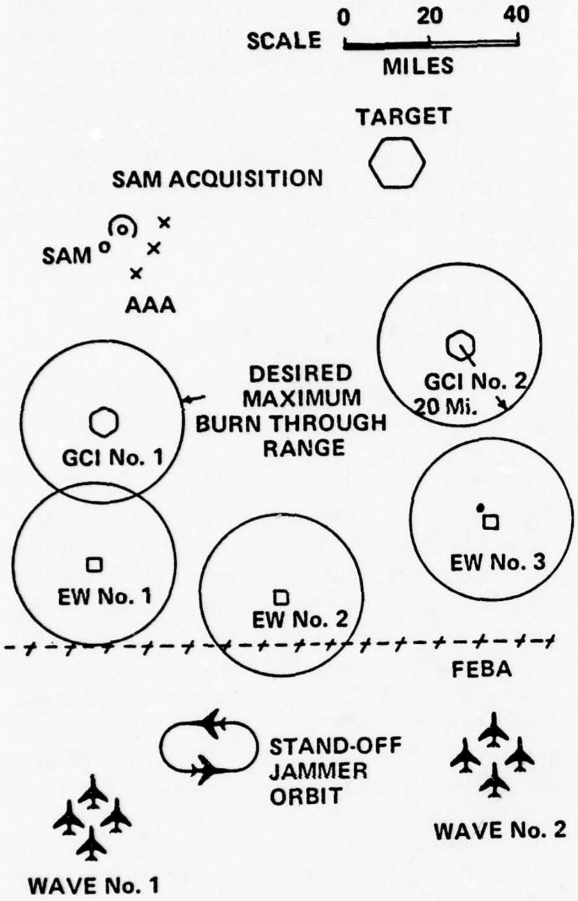


FIGURE 26. THE EFFECT OF STAND-OFF JAMMING ON TACTICAL AIR DEFENSES

reduced the geographical area coverage available to the defense.

On-Board ECM. Having accomplished the degradation of the EW and GCI net which normally feed acquisition information into the tracking radars of the SAM and AAA,[21] WAVE #1 clearly will have a lower probability of acquisition, P_a, by the SAMs or AAA. From this it naturally follows that the probability of survival of the attacking aircraft will be raised.

We are now ready to examine the role of on-board ECM equipment. Such equipment typically might be:

RHAW Equipment – carried on-board each tactical fighter to inform the pilot when he is being illuminated by a radar.

Disposable Jammers – small, inexpensive jammers equipped with parachutes.

Jammers or Deceptive ECM.

Assuming that the SAM and AAA track radars have swept the sky and have finally acquired WAVE #1 sometime after burnthrough, let us from this point discuss the noise and deception techniques for improving the probability of survival, P_s, which has already been improved by P_a. The SAM and AAA now are in the process of singling out the victim aircraft to attack.

Deception, as the name implies, is a technique for deceiving the tracking radar. For example, deception can force the victim radar, either by active radiators or chaff bursts, to believe the aircraft is slightly displaced in range and in angle from its actual position. Having accomplished this deception, which takes in the order of seconds, the tracking radar soon discovers what has happened and is forced to reacquire, most probably in the degraded manual track mode. In other words, you have broken his track and he must pin you down again.

On the other hand, jamming attempts to overpower the radar signal with another signal. When an aircraft is illuminated by a radar, for this example say a tracking radar, it reflects a certain portion of the energy; and, the elapsed time between transmission and reception is measured to determine range. If we employ a noise source covering the frequency band of the victim radar, say a portion of the E-Band, and broadcast a hundred times more power than the target would normally reflect (for example one-half watt per megahertz), the victim radar scope presents a strobe (a bright line at the bearing of the jammer revealing angle but denying range). The most satisfactory alternatives open to the sophisticated victim in such a situation are:

1. Triangulation: With the assistance of another radar, the victim radar may triangu-

[21] It might be useful to regard acquiring with a tracking radar without the benefit of prior position information as being analogous to trying to locate a bird in flight by looking through a megaphone.

late, determine range, and fire. If there are two attacking aircraft, an attempt at simple triangulation using two companion radars will obviously result in four strobe intersections, only two of which represent actual targets. In the case of four aircraft the intersections resulting from triangulation increase to 16 with a resulting 75 percent degradation in the target determination process.

2. Home-on-Jam Missiles: This is commonly accepted as by far the better choice for the defender. The use of disposable jammers[22] casually dropped by an attacker (or sown by a large stand-off aircraft) which will slowly descend by parachute would severely hamper this otherwise favorable alternative, and for that matter, would serve to further disrupt Alternative 1.

Integration With Tactics. Having forced the air defense into delayed acquisition, we find the defenders who have finally acquired WAVE #1 frustrated by on-board ECM and in a quandary as to whether they dare look around for another raid. It should be clear that with such degraded advance acquisition data, the AAA and SAM cannot slew[23] to new preinformed target positon.

When we consider these relationships, coupled with the fact that nonradar controlled AAA fire up the path of the tracers of radar controlled AAA, one can begin to appreciate the leverage that is gained in integrating an attack with a full complement of ECM weapons.

Electronic Warfare Design and Procurement

Having completed an overview of electronic warfare it is appropriate to consider how one ought to design EW equipment. Clearly an orderly design process starting with an initial concept and developing into an operational capability over a period of time would seem to be the desirable goal. However, two factors tend to interfere with this process. The first is the reactive nature of EW. If we have anything less than perfect knowledge of an enemy then we can expect to be surprised at some time. At that moment developing a counter has very high priority which leads to QRC procedures. Now QRC procedures not only short-circuit steps in the normal development cycle, they also contain less stringent financial controls because of the priority.

These "advantages", although necessary, tend to become addictive because they are easier; consequently more and more EW becomes funnelled through them. Thus major developments become funded through QRC, and the normal process atrophies. In effect we become so busy "firefighting" that we can never try fire prevention.

This process might be easy to stop in peacetime (in wartime it may be a moot point if there is a normal development process) if it were not for the second factor, intelligence. Because of the naturally occurring gaps in intelligence, electronic warfare developments are often targeted against ill-defined threats and thus are at a disadvantage in comparison to developments with more well-defined objectives. Thus EW developments may be delayed pending a precise definition of the threat. This delay insures that when and if the threat does become well-defined there will be a crash program (QRC, of course) to counter the new threat. Thus the lack of good intelligence tends to push all developments toward QRC.

The basic management problem then is how to guarantee orderly development of electronic warfare equipment and restrict QRC to the truely high priority items. For if QRC is abused by either funneling most EW development through it or by using it to routinely equip the force, it becomes "neither quick, nor reactive, nor capable".[24] One philosophical approach which has merit is to assume that in fact we will never have detailed

[22] Disposable jammers are small, inexpensive jammers, which at close range to the missile, will become stronger than the aircraft jamming and will attract the missile.

[23] Slew is a technical term for rapid movement of an antenna in azimuth or elevation to a new position.

[24] Harry I. Davis, "Avionics Systems: An Overview", (Lecture, Course 867.12, Avionics Systems Engineering, UCLA, July 1972).

technical intelligence until too late, thus our EW systems must be designed to be effective even when we are ignorant of important threat parameters.

This approach has at least two side benefits. First, planning for effectiveness in the face of gross uncertainty means that we may be able to guarantee a minimum effectiveness in the face of any threat. Secondly, this approach, being largely independent of precise enemy threat parameters may make us less sensitive to changes in these parameters. Thus we avoid the risk of massive failure of our equipment due to small changes in threat parameters.

There appear to be two methods of implementing this approach. One, which relates to ECM, is to use noise-like signals (jamming) in preferance to deception. The basis for this approach is that every system is susceptible to noise. The second approach is to make every equipment easily modified to meet the threat as it develops. This implies making transmitters and receivers which are capable to meet a whole spectrum of threats and which can be specialized or missionized to the particular threats without a complete redesign.

This philosophy is really a special case of decision-making under uncertainty and applies to all military developments. However, its necessity is made more pressing by the reactive nature of electronic warfare, and the normal lack of good technical intelligence in peacetime.

Electronic Warfare Evaluation

Now that we have looked at the general principles of electronic warfare, how do we decide how much to use, and how can we measure its effectiveness? Unfortunately neither of these problems admits to easy solutions. From the previous discussion we can state the following seven principles:

1. Our electronic warfare capability is no better than our intelligence, especially our electronic reconnaissance capability, be it ELINT, ESM, or RHAW.[25] To ignore the limitations of reconnaissance in planning ECM is to practice self-delusion.

2. The principle benefit of ECM is to secure a *relative* advantage over the enemy for a *limited* period of time, which may be quite long duration if the enemy is not on his toes.

3. The most ECM-resistant system is the one with the greatest number of optional modes of operation in the face of ECM.[26]

4. All other factors being equal, jamming is most effective when the penetrating force has a numerical advantage.

5. Deception (until compromised) is very useful in protecting single penetrators against terminal threats.

6. Well-integrated tactics provide effective ECM at critical points in the mission.

7. ECM must always be evaluated against alternative methods of accomplishing the same result—survival of the penetrating force. This means that ECM does not exist by itself and for itself but in active competition with other techniques. The best example of this was mentioned previously: Low altitude penetration is often very good alternative to ECM penaids.[27]

The Intangibles of EW. Having made this point we must also recognize that electronic warfare evaluation is also clouded by many intangibles. Electronic warfare itself is often surrounded by a shroud of mysticism because "the electrons cannot be seen." This aura of mystery is compounded by the fact that the ultimate objective is to affect a man, be he a radar operator or defense commander. The effect of these intangibles is difficult to

[25] Note that intelligence and electronic reconnaissance are not synonymous terms. But barring possession of equipment manuals, intelligence has limited capability of determining electronic parameters outside of ELINT. Thus electronic reconnaissance is usually the backbone of that intelligence useful in electronic warfare.

[26] But using the optional modes usually degrades system performance. See the discussion under ECM and Systems Operation earlier in this chapter.

[27] Mission profile and ECM are independent variables which may aid or oppose each other in the total effect on penetration. For example, low altitude penetration may be degraded by improper ECM. In general both must be considered in determining optimum penetration methods.

evaluate so we will content ourselves with a brief discussion of some of the more important ones.

One of the intangibles which affects electronic warfare is the psychological effects of ECM on the enemy. These effects are often cited as justification for ECM, but they are very hard to quantify. For example, a subject in a simulator experiencing ECM does not have the same psychological background as the airman in combat who knows that if he does not do his job a bomb or a bullet may come his way. Likewise, the evaluation of various "hunter-killer" concepts[28] often becomes the evaluation of a visceral feeling with the weighting depending on the attitude of the evaluator. Statistically, these concepts can easily lead to a higher loss rate for the hunter-killer teams. Is this higher loss rate offset by a greater effectiveness on the part of the remainder of the force? Reliable data to support an evaluation of this tactic is very hard to come by–combat is no place for precise data recording and maneuvers or tests just do not have the psychological drive.

Another intangible factor is that in combat success often goes to the innovator, the person who does the unexpected. The examples of this are legion; a current one is the use of the C-47 Gooney Bird in Vietnam as a gunship. Ten years ago how would you have evaluated the effectiveness of that airplane as a weapons system?

A corollary to this factor is the effect of long lifetime in electronic equipment. If a piece of radiating electronic warfare equipment has been in use for a long period of time then the probability is fairly high that the enemy knows about it and has developed a countermeasure. Hence, its most effective use in combat may well be some use completely different from its intended use. Such use of any equipment is difficult to predict, and one concludes that the most valuable characteristic of electronic warfare equipment is flexibility. It appears that we should concentrate on providing the commander with as many options as possible in his selection and use of electronic warfare and let him choose which one seems best in his situation. Of course, this implies that the commander and/or his staff are well trained so that they can make intelligent selections.

This discussion of intangibles is a reflection of the fact that ECM is basically a two-sided game with both sides actively seeking to gain the advantage. Any evaluation which ignores this fact is bound to give all the initiative to one side, our side. The result will invariably be favorable to our cause. Such results are useful only if they are used to compare different options, but invariably we come to believe that the figures are some absolute measure of our own invincibility. Hence we tend to become mesmerized by the results of our studies and disregard all results to the contrary. It then takes a combat situation to awaken us from our euphoric dreams and that may be too late.

Thus as in all warfare, ECM must be practiced and tested at all levels of training up to and including full-scale maneuvers. And if the results are not encouraging they should not be suppressed, but used rather as goads to developing an effective electronic warfare capability.

Electromagnetic Conflict and *the Learning Curve*

Having looked at electronic warfare from both the operational and technological viewpoints, it would appear that our discussion of basic concepts is complete. But as so often happens, one of the most important concepts is so often referred to and is so close at hand that it is easily overlooked. We refer to the man engaged in electromagnetic conflict, how does he interact with this part of warfare?

We have already made statements as to the value of well-trained operators in electronic warfare, the same applies to commanders. But how does a person become well-trained and how do you describe the benefits to be derived from training?

It appears appropriate at this point to introduce the concept of the "learning curve". This concept states simply that a

[28] Concepts which attack the defenses directly in an attempt to destroy them or, failing that, to suppress them or reduce their effectiveness.

man's performance of any new task initially shows substantial improvement with time, but as he becomes more skilled the rate of improvement slows down and his performance approaches a limiting constant value. This principle is so universally observed that it would be very surprising if it did not apply to electronic warfare.

The learning curve applied to EW says the electronic warfare capability of any man in a military force will follow a learning curve. If he trains extensively or experiences a long period of EW conflict, he will be well skilled or proficient, i.e., well up on the learning curve. If he has little experience, he will be unskilled, well down on the learning curve. This simple principle has several implications for a military force.

1. If the conflict is to be short and decisive, then our combatants must be well up on the curve, well-trained. Otherwise, the time required to obtain overwhelming proficiency may either prolong the conflict or invite defeat. Since we usually associate strategic warfare with short, decisive conflicts, this says that the operators and commanders in our strategic forces must be trained to the level of maximum competence or we invite defeat.

2. On the other hand, if we anticipate long, slowly-escalating conflicts, then our EW training can be minimal, because our commanders and operators will have time to train on the enemy tactics. This approach assumes that no decisive encounters will take place initially. This concept seems to fit our recent Southeast Asia situation and might be termed tactical warfare.

3. One of the implications of QRC development is that the operators never receive any initial training on the equipment. Thus all operator training tends to be on-the-job (OJT). In peacetime, this is acceptable but in wartime it becomes OJT in combat both for systems operation training and tactical employment training.

4. If we want EW to be effectively employed, our commanders must be trained beforehand. This implies a continuing program of EW education and training in peacetime. If this is not done, then the EW training must be obtained in combat. The corollary to this is that if we only train in combat, then we will preforce repeat all the mistakes we have made in previous conflicts in the process of relearning the correct principles. Needless to say, this latter principle is supremely important: we cannot expect EW competence in battle if we don't train in EW beforehand.

In summary, setting forth and understanding the academic EW principles is good but not sufficient; we must train with them before they will yield supremacy in battle.

Chapter 4

ELECTRONIC RECONNAISSANCE

Introduction

Although ECM has received the most emphasis in the open literature on electronic warfare, it should be clear that a prerequisite to ECM is knowledge of the enemy electronic systems. Hence, an intelligence function must precede all other aspects of offensive electronic warfare operations. In terms of the JCS definitions given in Chapter 1, this function would be called electronic warfare support measures or ESM. But as Chapter 3 shows, this definition, especially as it is embodied in military operations, is still too narrow, for it only covers the operational factors of what equipment is the enemy using and where; it does not cover the intelligence function which allows us to design our ECM equipment with good confidence that it would be effective against specific enemy systems.

In this chapter we want to address this intelligence function in the broadest possible context. Thus we wish to include all the categories of Table 7; that is, we wish to discuss electronic reconnaissance, the sum of all our efforts to gain information on the enemy systems which radiate electromagnetic signals. In so doing, we shall spend more time on the traditional intelligence functions of SIGINT (Signal Intelligence), ELINT (Electronic Intelligence), and COMINT (Communications Intelligence) than on the operational functions of ESM and Radar Homing and Warning (RHAW) because it is the former that provide the avionics that the commander can use in his tactical situation.

Another reason for adopting this approach is that ESM is a new term, being initially defined around 1969, and RHAW is a relatively new concept, having been extensively developed during the Vietnam conflict, although precurser equipment has existed for some time. With the relative newness of both these terms the technical concepts associated with them have not had time to become well defined. Hence, all their implications are not clear, and may not be clear for some time.

Traditionally, electronic reconnaissance has gone by the names of ELINT, COMINT or SIGINT. SIGINT, however, even though it includes COMINT and ELINT is not usually discussed in detail (although the intercept techniques are common for both ELINT and COMINT) because the operational controls on the resulting information are vastly different, depending on its derivation. COMINT implies the principles of encryption and decryption discussed in Chapter 7, consequently it is very closely held by any government because of the great value and extreme sensitivity of the information gained thereby. ELINT, however, uses information that is "public property" in that once a signal is radiated it is available for anyone to detect, so that information gained thereby is much less sensitive. Consequently SIGINT has become only a generic term for the results of intelligence based on radiated electronic signals with detailed discussion being titled ELINT if it concerns signal intercept and COMINT if encryption in involved.

From the foregoing discussion, it should be clear that COMINT cannot be meaningfully discussed *per se*; however, we can discuss separately intercept principles under the heading of ELINT and encryption-decryption principle under the heading of communications security. This is the procedure we have adopted, so that henceforth we shall talk exclusively about ELINT as the intelligence function of electronic reconnaissance.

Before we begin a discussion of the techniques and problems of electronic reconnaissance it seems appropriate that we consider the historical development of this field to obtain some perspective. Following that, we will consider first the characteristics of the enemy systems and then the basic principles of electronic reconnaissance. Analysis of reconnaissance data is a three-stage process, so we will discuss next the three stages of data collection and the information which can be derived from each stage. At that point we are in a position to discuss what requirements this data collection process places on the equipment. Having surveyed the breadth of electronic reconnaissance, it is appropriate to discuss the problems of reconnaissance and to illustrate the reconnaissance process by constructing a hypothetical reconnaissance mission. Finally we shall discuss ESM and RHAW.

Early Electronic Reconnaissance

Electronic reconnaissance is as old as the first military receiver, for clearly any commander wants to know what his enemy is doing and if the enemy is doing it as well as he is. Chapter 1 notes some of the early German and British efforts in this area. It should be obvious that given the cold war there is little incentive for any of the major powers to slacken their efforts in this area; although it is difficult to find information concerning current efforts in the open literature because governments are naturally reluctant to broadcast their successes or failures. But occasionally some information surfaces which indicates the importance of electronic reconnaissance.

The following extract from *"Electronic Intercept"* or *"Technical Search Operations"*: *History and Importance*, written in the early 1960s will give some of more recent historical background of electronic reconnaissance. (The footnotes have been provided by the editor).

> "Electronic intercept (ELINT) goes back to the days before World War II. To our knowledge the first ELINT mission at radar frequencies was conducted by the Germans. In mid 1939, prior to the outbreak of war, the Germans were desperately curious as to whether the British had radar. To find out, General Martini, then a colonel, used a Zeppelin as a ferret platform. He covered the English Channel and the Irish Sea areas for a brief period but his equipment was defective. For this reason, German intelligence drew the conclusion that the British had no radar. This illusion, all based on defective receivers, continued for some time. The moral as to equipment condition is obvious. Also, the merit of endless patience in collection is shown. Martini should have tried more than once. A single negative mission never justifies a conclusion.
>
> The British, of course, were wartime champions at collecting the really important data. The most famous British story concerns the discovery of the German Lichenstein A. I. As a result of this discovery timely and effective ECM was developed which negated a vital weapon of the Luftwaffe at an early date. So important was this in winning the "Wizard War", that Churchill in his history of the struggle describes the events in great detail.[1] To gather the data, a slow vulnerable British aircraft flew missions after mission over Germany inviting AI attack from night fighters. After literally months of frustration, the British were successful in luring the proper German fighters. As the bullets struck operator, aircraft, and equipment alike, the British took the priceless recording and measured the radar frequency and all other details. Persistence and patience in collecting ELINT are the moral of this tale.[2]
>
> Around 1950, the biggest debate in all our National Estimates on electronics and air defense was whether or not the Soviets had AI radar. The Navy, Air Force, and CIA would debate for hours on this

[1] Winston S. Churchill, *The Hinge of Fate* (Boston: Houghton Mifflin Company 1950), pp 278-279.

[2] *Ibid.* Chapter 16, pp 277-289 records several electronic warfare actions in Wold War II.

vital key to Soviet air defense capability. The rather vague rumors and reports of tube developments were inconclusive, as were the ELINT data. One attempt to solve the problem involved a Navy aircraft in the Black Sea, an incident which was oddly enough, well described by the Alsops in the *Saturday Evening Post.*[3] Finally it was the British again who settled the matter with an excellent 20-second aircraft recording of SCAN ODD radar from a Soviet interceptor. From this date on, there was no doubt as to the Soviets having AI radar, and the frustrating and time-consuming arguments in preparing National Intelligence Estimates were considerably reduced.

Today the TOKEN, and its new variants STRIKE OUT, BIG MESH, and SLANT MESH, represents the very core of Soviet air defense. TOKEN made its first appearance at the key Soviet development field in Izmaylovo in Moscow in the fall of 1951. Obviously inspired by our AN/CPS-6, it shook our intelligence community to the core when it was seen. This was the first Western-inspired equipment which was not a lend-lease radar. It was a modern set, comparable at that time to our very best radar. It was five high-power radars in one; and microwave to boot. Prior to that time, estimates of Soviet air defense gave them only GCI or fighter vectoring capability equivalent to that provided by an old 200-megacycle lend-lease radar.

The skeptics had their day on seeing TOKEN's antenna. How do we know it is not a dummy? The Soviets are masters of deception. Could this all be a false front, like the famous Russian Potemkin villages? Even if a radar, did it have five beams, or two, or one? ELINT gave us the answer. An attache sighted one of these "dummies" on the Polish Baltic coast. A British ELINT station was thus permitted to train a high-gain ground antenna on the Polish target from north Germany.

One evening a British specialist, assisted by a US Naval Research Laboratory Engineer, got the signals and established that five separate beams were coming from the radar, that the frequencies were similar to our own, that each beam had a common PRF, that rotation rates were synchronized, that peak power was obviously high, and determined the basic equipment parameters. This information was obtained only 4 months after the first prototype was seen in Moscow.

It was ELINT that first taught us how well the Sovets spread their equipment after they have decided upon an electronic system. The skeptics still had their day. Yes, they said, the Soviets have copied our CPS-6, but they cannot produce them in the numbers we can, nor can they maintain them. Within 6 months we had the answer to this fantasy. US Navy ELINT established that a chain of six to eight TOKENS was located on the Black Sea littoral. ELINT in central Europe located numerous others. And by June 1952, slightly over 6 months from initial discovery, spread of the equipment was apparent in the Soviet Far East. Based almost entirely on ELINT, within a year we had verified that the Soviets had far more TOKENS than the United States had CPS-6 radars. Not only did this informa-

[3] Joseph and Stewart Alsop. "Is This Our Last Chance for Peace?" *The Saturday Evening Post* (June 27, 1953): p 66.

tion help our National Air Defense Estimates, but it told us they could maintain the radars as well as or better than our technicians could maintain ours. This very unpleasant warning was given to us by ELINT 6 years before Sputnik number one. If the lesson was not learned it was not the fault of ELINT.

ELINT gave us a very good warning of Chinese Communist intervention in Korea. For about 2 years prior to our surprise on the Yalu, the Air Force and Navy conducted very regular search of the Chinese coast. The most prominent radar was always a high-power 100-megacycle set with wide pulses–quite obviously an effective US SCR-270. This was located in Shanghai, and regularly was heard hundreds of miles from our B-50s and P4Ms. In September of 1952 this radar disappeared from Shanghai. In October its high-powered signal suddenly was detected by ELINT from B-50s at Antung, on the Yalu River. We had a strategic warning of about a month–given to us by ELINT.

The Korean war was a wonderful stimulus to ELINT. We then had the support of those whose very lives depended upon jamming a Sino-Soviet SON-2, or "Elsie" radar. The fact that we were caught without satisfactory jammers in early stages of conflict was no fault of ELINT. ELINT and electronic intelligence personnel had been reporting Soviet block preoccupation with low frequency radar ever since 1947. In fact, it can be argued with good support that the intelligence was far superior to the ability of our planners to use it.

Most of the splendid strategic ELINT has resulted from specific operations designed against a very specific radar or technical target. A good example is the success of ELINT against the passive ECM device nicknamed BOX BRICK. Although suspected of being a radar search receiver/D-F, BOX BRICK was really somewhat an enigma. The British concentrated on the most vulnerable of these early sites, one in Austria. Careful ELINT coordinated with ground observers [and] with time coordination of observation, established that BOX BRICK did not radiate. Further studies using British active airborne and landbased radar in both S- and X-band in a similar fashion verified the activity of the device against our radar emissions, and even determined the intercept range of BOX BRICK. This little operation was one of the finest examples of British aplomb in the field of ELINT. The performance of this equipment is one of the few firm facts we have on Soviet operational ECM capability today.

In long-range navigation, the first proof of operations of a German-inspired Soviet low-frequency Loran came from ELINT–again British. This still represents a basic long-range navigation capability. As early as 1949, the mushroom in the IL-28 bomber was tied down by ELINT. The existence of very low frequency emissions from the Soviet block, of such great interest to our Navy in studying Soviet submarines, were verified on the same day by the United States and British ELINT units. This occurred some 3 years prior to photography of the Soviet copy of the German GOLIATH transmitter near Gorkyy. Case after case of comparable ELINT contributions to our overall estimates may be cited. . . .

A word of caution is in order, however. ELINT should not be regarded as an end in itself. Powerful tool that it is, it must be coupled with a balanced program of collection and analysis from other sources: photography, open literature, defectors, returning workers, visitors to the Soviet Union, captured and examined equipment and documents. ELINT is just one part of the overall contribution to intelligence on Soviet electronics. The ELINT specialist should not become so specialized that he is unaware of these other sources or allow himself to become separated from the whole of which he makes a part.

It is interesting to note that the ELINT operations which really made vital contributions to our overall appreciation of Soviet electronics had two things in common. They were generally conducted by persons who were far more than narrow specialists–by people who had the "broad picture." Also, they were directed against a specific target, with a specific goal and a specific plan.

The future of ELINT is far brighter than its past. In the future ELINT may determine many matters. Success against Soviet [radar] jamming signals, . . . success against the elusive Soviet submarine radar SNOOP PLATE, far more data on missile-connected systems, detection of extremely long-range warning radars, and detection of many other unusual and fantastic devices are all probable. The secret of success remains competence at the operator level. Despite the rumored emergence of the machine "brains", the human being remains the vital component in our ELINT, as in other fields."

It is difficult to obtain any recent information on ELINT since the day-to-day activities are not usually revealed. Nevertheless, one can appreciate that open or covert "snooping" for electronic emissions is not always appreciated. Every so often, a country becomes provoked at such missions and resorts to bullets to discourage the practice. At such times the results are reported in the press. Of course, such results also illustrate the hazards involved in electronic reconnaissance. That such hazards are real is shown by a selected list of such events as reported by the New York Times (Table 13). Figure 27 plots the location of the events recorded.[4]

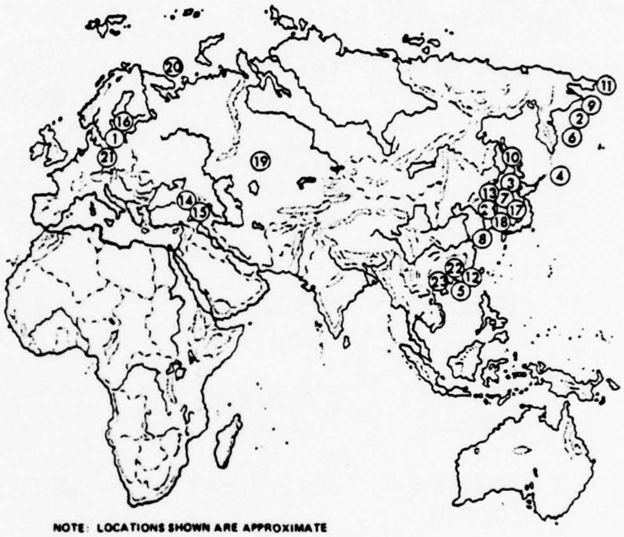


FIGURE 27. AIRCRAFT INCIDENTS

Enemy System Characteristics

Before we discuss electronic reconnaissance further it may be helpful to consider the enemy equipment being electronically reconnoitered. A listing of its characteristics will serve to highlight some of the objectives and problems of reconnaissance.

a. *It is a system.* We must realize at the outset that we are interested in enemy systems, not in enemy signals *per se*. It is only as we can relate the particular signal to a system that we have gained any information of *military* significance. It is true that a new signal, say at a previously unobserved frequency, will tell us that the enemy has a scientific or technological capability

[4] Pali, *Technik und Methoden*, pp 328-337 also discusses electronic reconnaissance and illustrates its hazards.

Table 13

Aircraft Incidents

Date Published (Occurred)	Location	Aircraft	Results/Survivors
1. 12 Apr 50	Baltic Sea	Navy Privateer (USSR alleges B-29)	Shot down by Soviet fighters, no survivors, life rafts & aircraft parts found with bullet holes. Four Soviet fliers lauded by Stalin. Reported in 1955 that eight crewmen may be in prison camps
2. 6 Nov 51	Off Siberia	USN Weather Reconnaissance	Shot down by Soviet fighters, 10 missing
3. 13 Jul 52	Sea of Japan	B-29	Disappeared, crew of 13 missing
4. 7 Oct 52	Kuriles	B-29	Shot down by Soviet fighters, no survivors
5. 19 Jan 53	Off Swatow, China	USN Neptune	Shot down by Chicom fighters, two missing, 11 survivors
6. 18 Mar 53 (15 Mar)	E of Kamcnatka Peninsula	RB-50	Attacked by Soviet MIGs, no damage
7. 31 Jul 53 (29 Jul)	Sea of Japan	B-50	Shot down by Soviet fighters, one crewman recovered, 16 missing, some may be held by USSR
8. 22 Jan 54	Yellow Sea	RB-47 & F-86	Attacked by eight MIGs, no casualties
9. 6 Sep 54 (4 Sep)	Off Siberia	USN P2V Neptune	Shot down by Soviet jets, nine crewmen rescued, one missing
10. 8 Nov 54 (7 Nov)	Hokkaido, Japan	RB-29 Photo-reconnaissance	Shot down by two Soviet MIGs 10 crewmen safe, one dead
11. 25 Jun 55 (22 Jun)	Bering Strait	USN P2V-5	Attacked by Soviet fighters, crash-landed on St. Lawrence Island, three hurt by gunfire, four injured in landing, remaining four unhurt
12. 23 Aug 56	E China Sea	USN P4M Mercador	Shot down by Chicom fighters, 16 crewmen missing
13. 17 Dec 56	near Vladivostok	3 B-57	USSR charges violated air space

Date Published (Occurred)		Location	Aircraft	Results/Survivors
14.	29 Jun 58 (27 Jun)	Armenian Republic	C-118	Shot down by two Soviet MIGs, nine crewmen returned
15.	13 Sep 58 (2 Sep)	Armenian Republic	C-130	Shot down by two Soviet MIGs, six dead crewmen returned, 11 others missing. (Have tape recording of fighter conversation, suspected meaconing)
16.	18 Nov 58 (17 Nov)	Baltic Sea	RB-47	Attacked by MIGs from USSR. No damage, no casualties
17.	18 Nov 58 (17 Nov)	Sea of Japan	RB-47	Attacked by Soviet MIGs, no damage, no casualties
18.	17 Jun 59 (16 Jun)	Sea of Japan	USN Patrol craft, reconnaissance	Attacked by two MIGs, tail gunner hurt
19.	6 May 60 (1 May)	Sverdlovsk	U-2	Shot down by SAM, pilot released in 1962
20.	12 Jul 60 (1 Jul)	Barents Sea	RB-47	Shot down, four crewmen dead, two crewmen held and tried in USSR, later released
21.	11 Mar 64	E Germany	RB-66	Shot down, three crewmen released within month
22.	8 Feb 66	Communist China	Reconnaissance drone	Shot down
23.	1 Apr 66	S China	KA-3B Tanker	Shot down
24.	16 Apr 69	N Korea	EC-121	Shot down, 31 crewmen dead

NOTE: Data obtained from the *New York Times Index*.

previously unobserved, but unless we can relate that signal to a system we can only postulate a military capability. One would not be surprised if our reconnaissance files had many signals which, having been observed only a few times and being unrelated to any known system, have no intelligence or electronic warfare value.

b. *The system is man-made*. There are many natural sources of signals, thunderstorms being one of the most common. These naturally occurring signals, while they may interfere with military operations, are not controllable by the enemy, hence they are of no interest to our electronic reconnaissance. We are interested in signals which are deliberately generated by man. This characteristic immediately gives us one method of discrimination, for the natural signals are random and noise-like while man-made signals usually have some repetitious character which we can use as an identifier. Hence, reconnaissance involves separating the man-made signals from the noise.

c. *The system has integrity*. By this characteristic we mean that all parts of the system contribute to the common goal. Hence two different signals emanating from the same system must support a common purpose. Likewise if the system is known then the purpose of an observed signal can be inferred.

In this connection we must observe that unintentional radiation may not be purposeful but it still can give us information about the system. For example, it is well known that TV receivers tend to radiate the local oscillator signal. The radiation of the signal is not intentional, it is a consequence of inadequate shielding in the receiver. Thus, if you receive such a signal from a house you can infer that the occupants are watching TV and from the signal frequency you can deduce which channel. That is, given sufficient data from monitoring that signal you can gain a good picture of that family's TV habits and preferences. (This is exactly the method used by some TV rating services and a court has ruled that such monitoring is not an invasion of privacy.)

d. *The system is large*. If the system radiates a signal then it has considerable size in some aspect: in number of different parts, in functions performed, or in cost. This means that there are many approaches and levels of analysis which we might undertake, depending on our objective. Thus our analysis of our reconnaissance findings will probably be limited by cost or exhaustion, not by a lack of things to know.

e. *The system is complex*. This characteristic is one consequence of a large system. But the effect of the complexity is to make the interrelationships between system variables complex and usually nonlinear. Thus a change in one variable is likely to be reflected in many other variables, often in non-linear form. This makes our analysis of the observed signals difficult, especially if we are interested in the root causes of the observed changes and their implications on system function and performance.

f. *The system is semiautomatic*. Most military systems involve both men and equipment. so both automatic functions and manual functions are expected. We would like to separate the two through electronic reconnaissance. However, men do not radiate strong signals so the manual functions may have to be inferred or obtained by other means.

g. *The system inputs are stochastic*. This is one of the major differences between testing and reconnaissance. In testing the system inputs are known beforehand–*a priori*. Thus the ensuing behavior can be correlated with the known inputs. But in reconnaissance the inputs are usually unknown so we cannot predict the exact load or performance of the system at any moment. Thus the reconnaissance output is characterized by average values with a measured distribution about the average.

This stochastic nature arises not only from the unknown conditions among the enemy but also from the unknown and uncontrolled variability of our own equipment. Hence, it is important for good reconnaissance to have good equipment whose characteristics are well defined, so that we can separate out the effects due to measurement from those due to target system operation. Unfortunately the airborne environment is one of the most severe and difficult to control both due to size and weight constraints and to vibration and other environmental factors. Thus good reconnaissance equipment is usually very expensive.

h. *The system is competitive*. By this we mean that the enemy considers any deployed military system better for its primary mission than all other competitive systems. And our analysis of our reconnaissance is not really complete until we have understood the reasons why the enemy thinks the system is competitive. History is replete with tactical and strategic surprises which occurred because the enemy's reasons for using a system were not understood. The Trojan Horse is probably the most classic example.

In summary, our electronic reconnaissance must recognize and account for these characteristics of the enemy systems if it is to be successful. Unfortunately, since our information is often very imperfect and incomplete, many conclusions must be based on inference. As a result it is quite possible to reach two different conclusions from the same data. If further data is received one can in some cases resolve these conflicts. But inference is easily biased by the implicit assumptions of the analyst, so that occasional failures of electronic reconnaissance should not be surprising even though they may be regrettable.

The Basic Principles of Electronic Reconnaissance

As the previous history has documented, electronic reconnaissance is a valuable, continuing, and hazardous operation. Consequently, there are several operational principles which must be observed in such missions in order to collect the necessary data.

1. *The electronic environment must be stimulated so that the desired signals are transmitted.* Unless the enemy perceives some essential threat, he may never turn on the transmitters we are interested in, preferring to take the remote risk of attack to that of revealing some facet of his operational capability. Thus electronic reconnaissance often resembles a cat-and-mouse game.

2. *The provocation must be consonant with national and/or military objectives.* One can appreciate that stimulating the enemy to exercise his electronic environment in times of great international tension could possibly provoke armed conflict. Hence the cat-and-mouse game must be played with an understanding of the possible repercussions. The Powers U-2 incident (Item 19, Table 13) is a case in point. As a result, reconnaissance in an armed conflict is likely to be bolder and easier than in peacetime where the enemy options are greater and more uncertain.

3. *The reconnaissance coverage must seek both to discover new developments and confirm previous knowledge.* One can easily appreciate that reconnaissance wants to know and investigate all new equipment which appears in an enemy inventory. But it is also important to know that the enemy disposition of forces, the electronic order of battle,

Table 14

The Characteristics of the Three Types of Reconnaissance

Major Items	ELINT	ESM	RHAW
Environment Stimulation	Low	Medium	High
Provocation	High	Medium	Low
Coverage[1]	Infrequent	Frequent	Frequent
New	Good	Fair	Poor
Existing	Good	Good	Fair[3]
Immediate Evaluation and Response[2]	Poor	Fair	Good[3]
Long Term Analysis	Good	Fair	Poor

[1] Rated both by the frequency of coverage and the technical capability to determine signal presence.

[2] Rated by the ability to convey the information gained to the user.

[3] Within its capability, RHAW is designed to permit the aircrew to evaluate and respond immediately to signals within its detection capability

is unchanged. So electronic reconnaissance must periodically return to an area to confirm previous data.

4. *Electronic reconnaissance must have the capability of both immediate and long-term analysis and response.* Since the collector is often covering the same geographical and spectral regions repeatedly, many of the signals intercepted will be signals known to be there by previous efforts. These signals require minimal collection effort. But new and unusual signals require immediate action both to obtain technical information and to respond to any implication as to enemy capability.

In addition to these principles, we must remember the one major limitation of electronic reconnaissance: it can only observe signals which are radiated by the enemy. If the enemy has passive systems, systems which receive the signals emanating from our aircraft, no amount of electronic reconnaissance *per se* will detect their existance or reveal their characteristics. To determine the parameters of passive systems, we must turn to other forms of intelligence. And unless we obtain specific technical data we can only presume a capability, for even photographs of the equipment exterior may not reveal its capability. Consequently, estimates of the capability the enemy's passive systems must usually be based on the educated guess that potentially he should have that capability.

These four principles apply in different degrees to the three areas of reconnaissance. Table 14 generally classifies their application.

The Stages of Data Collection

The actual collection of electronic reconnaissance is a three-stage process. The first stage is to obtain the new data, the actual observation of the signal itself. The second stage is to analyze this raw data to infer other characteristics of the equipment producing the signal. At the same time the received signals must also be analyzed to determine the intentions of the enemy concerning the collector. Finally, in the third stage, this information is collated with that derived from other sources to achieve the end product—scientific and technical intelligence, order of battle, threat information and operational intelligence. Let us expand this concept a bit.

Raw Data Collection. Each equipment or site which radiates electromagnetic energy has its own "fingerprint" which can be intercepted and recorded. The energy from a particular equipment will be called a *signal.* The basic information which a receiver can determine from a signal is the following:

a. Received power—which depends upon the distance and orientation from the transmitter.

b. Signal Spectrum

c. Signal envelope

d. Time variation—these are the gross variations due to antenna scan[5] or transmitters being turned on or off.

e. Signal polarization—the orientation of the electric field in the signal.

f. Direction of the transmitter from the receiver.

The above description sounds simple but it is complicated by the enormous number of electromagnetic signals which exist. One must first sort out the interesting signals from all the others. These are usually the new or unusual signals or familiar signals which have changed. Thus many of the received signals convey no information, so that the collector must collect and sift through enormous quantities of data to find the desired information. Many times it is literally like looking for a needle in a haystack.

To this problem one must add the uncertainties of propagation, of enemy and friendly operations, and of equipment maintenance and calibration. For example, in the frequency bands above HF where line-of-sight propagation is the usual mode, much information is denied because the proper collection equipment cannot get close enough to the transmitter at the time the transmitter is operating. In fact, through surprise, the enemy may deliberately capitalize on this uncertainty to prevent us from getting good

[5] Scan is the motion of the antenna radiation pattern which may be caused by mechanical motion of the antenna or by electronic techniques. See Chapter 2.

information on a piece of new equipment he has to expose to us.

These considerations have led to the following three principles of ELINT collection, which are an expansion of principle four, above.

5. *Collection must be accompained by on-the-spot preliminary analysis to determine if the data is worth saving.*

6. *Collection must be capable of rapid response to observe and record significant new data.*

7. Because *ELINT* is credible due to its immediacy and the enemy's ignorance of our possession of it, it *must be well protected and it must have fast channels of transmission to the interested users and commanders.*

Analysis. The components of the fingerprint which the collector would like to know are as follows:

a. Transmitted power
b. Carrier frequency
c. Modulation
d. Antenna pattern
e. Antenna scan
f. Transmitter location (range and bearing)

Some of these are easily inferred from the received signals. For example, the carrier frequency usually can be quickly derived from the spectrum. The type of modulation may also be determined from both the spectrum[6] and the envelope of the signal. If the antenna moves in a consistent fashion, such as a radar antenna, then the antenna movement (scan) may be determined from the time variation of the signal.

The other components of the fingerprint are more difficult to determine. To determine transmitter power the collector must know the distance from the transmitter to his receiver. The antenna pattern of a stationary antenna requires that he analyze the time variation of the received signal at a moving collection point. If computation equipment is on board the airplane then transmitter range and antenna patterns can be determined immediately. Otherwise this analysis must wait until later.

Threat Analysis. There is another type of analysis which must proceed simultaneously with the above signal analysis and which is concerned not with the signal parameters themselves but with the implications of these signals to the collecting aircraft. This analysis attempts to infer the state of the enemy reaction to the collector and thus the level of danger. For example, low PRF, low frequency signals imply only that the aircraft is under surveillance by an EW radar while strong, high frequency, high PRF signals imply that a tracking radar for some weapon is tracking the aircraft. In the former case the immediate threat to the aircraft is small while in the latter case the immediate threat is very high. RHAW equipment does some signal analysis automatically and presents the information to the pilot or operator in such a fashion that the threat is high-lighted. On every reconnaissance mission the operators must be aware of the immediate threat implications of the signals they are observing, since downed aircraft usually do not yield much ELINT.

Collation. The ultimate goal of electronic reconnissance is to determine the following information.

a. Equipment characteristics (scientific and technical intelligence)
1. Transmitter power
2. Antenna type
3. Frequency
4. Modulation
5. Special characteristics

b. Geographic location (order of battle)

c. Operational procedures (operational intelligence)

d. Equipment use and capability (the threat)

[6] With pulse modulation (a typical radar) the pulse shape (generally its width) determines the width and shape of the signal spectrum, and the pulse repetition frequency (PRF) determines the spacing between the lines of the spectrum. If the modulation consists of analog signals then the spectrum may have a characteristic appearance depending upon the particular modulation. However, the receiver characteristics will modify the appearance of the spectrum, and although the presentation may have a characteristic appearance, it may be impossible to determine precise modulation parameters from the spectrum.

e. Messages transmitted (COMINT)

The determination of the above information invariably requires further analysis of the data, including data from other collection sites.

Collating the data from one or more sources over a period of time (traffic analysis) gives electronic reconnaissance an important additional capability. For example one might count the increase or decrease in radio communications in a sector. With accurate measurement of the volume of voice radio calls each hour or each day it could be possible to forecast an enemy build-up, planned offensive, or withdrawal.

Electronic Reconnaissance Equipment

The basic problem of ELINT is obviously to obtain the new data upon which the three stages are built. To obtain this data the airborne collection station will have to have some special receivers. These receivers differ from ordinary receivers both in their essential design and in the auxiliary equipment associated with them. The essential design requirements are:

1. Wide spectrum surveillance
2. Wide dynamic range
3. Good unwanted-signal rejection
4. Good angle-of-arrival measurement.

The wide spectrum surveillance is required because we do not know, *a priori*, the frequency of enemy signals. With present technology this means we must be able to search the frequency spectrum from 30 MHz to 50 GHz. This range is too large for one receiver to cover so that either we must use several different ECM receivers with different tuning ranges, or we must modify one receiver by inserting different tuning units or "heads" to cover different parts of this frequency range.

The wide dynamic range requirement means that the receiver must be able to receive very weak signals and very strong signals *without changing its characteristics*; for we do not always fly at great distances from a transmitter, we may find ourselves flying very close. We do not want the resulting strong signal to disable our analysis capability.

The unwanted signal-rejection capability is dictated by the fact that many other signals will exist with frequencies close to the signal of interest. We desire that the receiver discriminate well between the frequency it is tuned to and signals at other frequencies. Unwanted signal-rejection is often specified by three terms: *Cross-modulation* characteristic, *intermodulation* characteristic and *spurious frequency* rejection characteristic.

Finally, the good angle-of-arrival measurement capability allows us to locate the transmitter by taking bearings at different times (different aircraft geographical positions). Plotting these different bearings on a map will locate the transmitter by triangulation.[7] An airborne or ground-based digital computer can also be programmed to perform the same function.

Although we have distinguished a reconnaissance receiver from an "ordinary" receiver in terms of its design characteristics, it often maintains the general character of a superheterodyne receiver. That is, the design features are embodied in its technical specifications, not in its basic organization. Appendix B discusses how these specifications can be realized by specific receiver functions.

Problems of Electronic Reconnaissance

There are characteristics of both the target system and the collection equipment that may sometimes make the analysis of collected data difficult. Each of these problems must be understood to properly use the results of electronic reconnaissance.

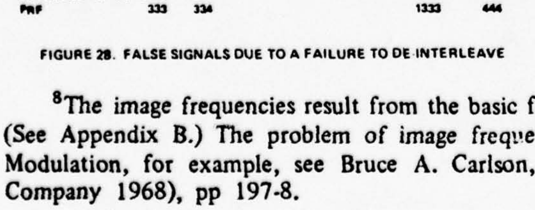
Equipment Problems. Certainly the utility of the data collected is a function of both the accuracy and the sophistication of the electronic receiver. *Receiver accuracy* derives both from the calibration of the reciever in the airborne environment and from operator proficiency. But the accuracy of the receiver establishes the basic accuracy in the values ultimately derived for the frequency, transmitted power, location, and other characteristics of an enemy emitter. Only by averaging the results of many observations can

[7] See Appendix B for a more complete discussion.

this accuracy be decreased. But such statistical techniques cannot supply data which the receiver is incapable of measuring. E.g., if the frequencies of two different radars cannot be resolved by the receiver, statistical techniques will give the average frequency, but will never tell us there are two separate radars.

The accuracy and reliability of the information collected on the parameters of the intercepted signals is also influenced by the receiver's tendency to produce *false signals*. For example, it is a well known fact that superheterodyne receivers have a tendency to respond to signals at their image frequencies.[8] Hence, it is possible to "receive" signals which do not exist unless the operator takes the proper precautions. The solution to this problem is best accomplished by a combination of good receiver design to reduce the image and spurious frequency response of the receiver, shielding to prevent any signals from entering the receiver except by the antenna, and operator training.

When collecting data in an environment that has many signals at or near the same frequency, it becomes extremely difficult to separate one signal from another for analysis purposes or identification ("*de-interleave*"). This problem is severe enough when radars at the same frequency in the search mode are "painting" the receiving antenna at different times. However, when the radars are in the track mode, they are "locked on" to the collecting aircraft and it is virtually impossible to separate one signal from another. Hence signal discrimination can be very difficult. This problem is most severe in RHAW equipment where the discrimination function may be mechanized by a particular algorithm. In this case one may obtain indications which range all the way from ignoring all signals to mistaking some signals for others. Figure 28 illustrates an example where inability to de-interleave creates false signals.



a. RECEIVED SIGNAL

ACTUAL RADAR:

	No. 1	No. 2
FREQUENCY (MHz)	1650	1652
PRF	333	334

b. RESULTS OF AN AUTOMATIC ANALYZER WHICH SENSES INTERPULSE INTERVAL

ANALYZER OUTPUT:

No. 1	No. 2
1650	1650
1333	444

FIGURE 28. FALSE SIGNALS DUE TO A FAILURE TO DE-INTERLEAVE

If shortcomings on the part of the collector, or cleverness on the part of the enemy defense, cause a signal of interest not to be seen frequently enough or with enough certainty to derive reliable information on that signal, then we have *incomplete sampling*. In this case either the aircraft must fly a pattern such that more data can be obtained on the signal in question, or collateral means must be used to derive the signal characteristics. Another consequence of incomplete sampling is that a new signal may not be distinguished from an existing signal so that the new signal is effectively "lost".

Analytical Problems. The previous four problems apply to the collection aircraft itself. They in turn lead to a problem faced by the analyst which can be termed *indeterminate causality*. The nub of this problem is that the analyst is unable to determine the sequence of events which resulted in the employment of the signals observed. The reasons for indeterminate causality are different depending upon whether the collection is done in a peacetime, "cold war" environment, or in a period of open, armed conflict. In a peacetime environment, the name of the game is to conceal your capabilities, hence the intelligence collector has very sparse information upon which to base his analysis. On the other hand, during open conflict the collector suffers from paucity in the midst of overwhelming data. Both sides are using all their resources to achieve supremacy. And

[8] The image frequencies result from the basic frequency conversion processes used in the superheterodyne. (See Appendix B.) The problem of image frequency response is discussed in any good text on Amplitude Modulation, for example, see Bruce A. Carlson, *Communication Systems* (New York: McGraw-Hill Book Company 1968), pp 197-8.

even though the enemy may expose many of his signals in response to air attacks, our emphasis is to win, not take data. Thus many signals may be observed, but which ones interact?

Indeterminate causality would not be a problem if reconnaissance were purely interested in the signals. But as we commented before, one ultimate goal of reconnaissance is to understand enemy systems. And lacking the enemy technical and operational manuals themselves, one way of understanding a system is to observe its reactions to different combat situations. In engineering parlance, we observe the system inputs, the signals which constitute our threat to the enemy, and the consequent enemy response to the threat, that is the enemy system outputs. Causality means that we can establish a cause and effect relationship, such a signal caused another signal, etc, and causality is essential to do this sort of systems analysis. But if the causality is indeterminate any analysis fails.

The result of these problems is that the analysis and collation functions may have a minimum of good data to work from. In an attempt to fill in the gaps the analyst may resort to the techniques of *simulation* and *inference*.

Simulation is the process of constructing an analytical model of the equipment being analyzed. The model is made to match the existing data and then it is exercised to determine other characteristics. For example, one might construct a model radar antenna from a photograph and then use that model to determine the pattern of the actual antenna.

Inference is the process of filling in the gaps in our intelligence by postulating either what we would do[9] or what we think the enemy might do.[10] The result is very dependent on our understanding of the enemy and can produce gross distortions of enemy capability.

In both these areas it should be clear that although the resulting picture appears to be *quite complete, the results are often* very subjective and no more accurate than the basic data. The problem is analogous to trying to determine whether you should date *the girl next door on the basis of* observations made through a double row picket fence.

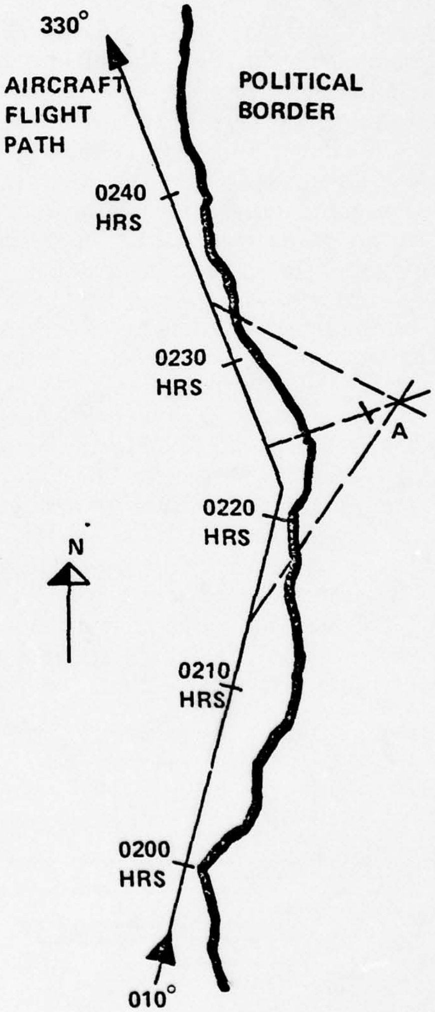


FIGURE 29. TYPICAL RECONNAISSANCE FLIGHT PATH

[9] This is often called the *mirror-image* problem.

[10] Usually our estimates of enemy capability are optimistic. Hence we tend to create a "10-foot-tall" enemy who is almost impossible to defeat.

An Example of Electronic Reconnaissance

Let us illustrate these concepts with a specific but hypothetical example, that of gathering data on a new enemy radar whose existence has been reported. The list of information which we want to determine (the collection requirements) is as follows:

a. Geographic location
b. Intended use
c. Radar range
d. Transmitter power
e. Susceptibility to ECM
f. Antenna pattern (beam width)
g. Antenna gain
h. Antenna polarization
i. Frequency
j. Frequency agility
k. Pulse width and pulse shape
l. Pulse repetition frequency (PRF)
m. Scan rate
n. Stability
o. Modes of operation

The Mission. The actual data on the enemy radar is obtained from an airplane flying along the enemy border on an ESM mission. Figure 29 shows the flight path of the airplane. The sequence of events as they might occur on the mission are as follows:

0200 hours - Aircraft true heading and true course 010°, altitude 30,000 feet, ground speed 500 knots, normal activity.

0208 hours - Faint buzz heard in Electronic Warfare Officer's (EWO) earphones.

0210 hours - Buzz repeats itself at 10 sec intervals. No other indications found as yet.

0212 hours - Pan adapter[11] shows a new signal centered at 2.54 GHz whose appearance coincides with the buzz. The signal lasts for about .1 second each time it appears.

0214 hours - DF bearing on new signal 017° relative to nose of aircraft. Signal is vertically polarized.

0215 hours - Although the audio signal has not changed a new signal has appeared on the pan adapter synchronized with the one at 2.54 GHz. Spectrum of new signal is centered at 2.91 GHz. (Signal characteristics suggest search/GCI/acquisition radar. Watch established for terminal threat signals – AI or SAM radar.)

0220 hours - Signal at 2.54 GHz has disappeared.

0223 hours - Course change to true course of 330° initiated. Signal at 2.91 GHz has same pulse width, PRF, spectrum width, DF bearing, and polarization as signal at 2.54 GHz.

0225 hours - DF (relative) bearing to signal at 2.91 GHz is 107°, aircraft true heading 325°. (SAM lock-on observed at 5.9 GHz. Navigator confirms position is 5 miles West of border. No visual sightings of missiles in flight.)

0230 hours - Sound of signal at 2.91 GHz has changed. Pulse analyzer shows that two different PRFs appear to be present. Signal is apparently switching back and forth between the two PRFs. PRF values are 300 and 325 pps.

0233 hours - Signals at 2.54 GHz and 2.91 GHz are of equal strength. Both signals show the two PRF phenomena. DF bearing is 152°

0237 hours - Signal at 2.91 GHz has disappeared. Signal at 2.54 GHz changes to a PRF of 325 pps.

0240 hours - Pilot reports sun glint off aircraft about 3 miles to right. Navigator confirms position 2 miles West of border. Aircraft is an interceptor type, judging from speed, but does not approach closer.

[11] See Appendix B.

Post-Mission Analysis. Once the airplane has landed the data obtained from the mission will be analyzed further. Analysis of the magnetic recording confirms the following data:

Frequency:	2.54 ± .02 GHz (receiver calibration accuracy) 2.91 ± .02 GHz
PRF:	300 and/or 325 ± 10 pps
Pulse Width:	5 μsec ± .25 μsec
Antenna Beam-Width:	4° (from the signal duration).

The spectrum width is consistent with the pulse width. A plotting of the aircraft track and the DF bearings (making allowance for the aircraft heading) shows that the signals all came from the vicinity of point A. Accuracy of location is ± 2 nm. Estimated effective transmitted power is 10000 megawatts.[12]

A calculation of the elevation angle of the airplane above the horizon at point A as it traversed its flight path produces Table 15. This data is interpreted to mean that the radar has two beams at the same azimuth but at different elevation angles and different frequencies. (Subsequent flights identify two more signals of different frequencies but otherwise similar characteristics coming from A.)

Table 15

The Results of ELINT Analysis

Elevation Angle	Signal Strength	
	2.5 GHz	2.91 GHz
0.5°	zero	zero
1.5°	maximum	zero
3.0°	equal	
4.0°	zero	unknown
5.0° (max)	zero	maximum

The two different PRFs imply that either PRF can be selected or that the radar can switch between them on a programmed basis (staggered PRF). This latter capability is indicative that the radar has the feature of a moving target indicator (MTI) which emphasizes only the targets which are moving radially with respect to the radar. Confirming this hypothesis is data received from subsequent flights which suggest that the frequency is very stable from pulse to pulse. This latter data also suggests that the MTI is a type known as coherent MTI, a capability which has been previously unobserved.

The presence of the SAM signal and the sighting of the (presumed) interceptor suggest, but do not confirm, that this radar is a GCI radar (i.e., it controls interceptors), that it passes acquisition data to the SAM system and that this radar is a new installation the enemy is anxious to protect. This further suggests that a continued collection effort in the vicinity of A might be worthwhile. Finally the time sequence of events suggests an interceptor *reaction time* (threat detection to interception) of 30 minutes maximum in the vicinity of A.

Information from other Sources. Several weeks later a photograph of a new air traffic control radar which has been installed at the airport near A is observed in an enemy magazine. In the background is another radar set and, although the picture is not clear, this radar seems to have more than one feedhorn illuminating the antenna. In fact, it appears that there are four feedhorns. The antenna size appears to be about 30 feet wide and 20 feet high.

A month later a report is received that considerable fighter traffic has been observed at the airfield near A. This report is considered not too reliable. Then two weeks later a station in the US monitors a message from an enemy HF station which, when decoded, refers both to the air defense sector including A and to the interceptor control station at A.

[12] This includes the antenna gain.

Scientific and Technical Intelligence. The consequence of all these facts is the following information:

Nickname:	LARGE BANG
Pulse width:	5 μsec
Transmitter Power:	1 Megawatt (transmitted power divided by antenna gain)
PRF:	300,325 pps singly or staggered
Antenna Gain:	10,000 (40 dB) (obtained from antenna dimensions)
Scan Rate:	6 rpm
Beam Width:	Azimuth 4°, elevation 3° all beams (obtained from a simulation of the radar antenna)
Number of Beams:	4 (a stacked-beam radar)
Beam Elevations and Frequencies:	1.5° – 2.54 GHz 4.5° – 2.91 GHz 7.5° – 2.67 GHz 10.5° – 3.05 GHz (obtained from a model of the radar antenna constructed from the photograph and collated with ELINT data)
Tuning Capabilities:	All frequencies can be varied ± 5 percent from the values given above (obtained from our estimates of enemy technology).
Elevation Change:	The beams may be varied ± 5 degrees in elevation from the positions given. The beams always maintain the same relative positions and frequencies. When the beams are lowered the transmitters for the lower beams can be turned off. (Data obtained from subsequent flights.)
Maximum Range:	250 nm (derived from PRF)
Location:	At airfield near A
Special Features:	Coherent MTI
Susceptability to Active EW:	Significantly improved because of the quality inherent in having coherent MTI
Intended Use:	As a GCI control radar associated with the air defense squadron stationed at A. Also as a possible acquisition radar for SAM sites near A.

Enemy Order of Battle. The enemy order of battle is also changed by the addition of a LARGE BANG radar at A.

Threat Evaluation. This radar not only represents an extension of the enemy's air defense structure westward but it also represents a significant improvement in his air-defense capability inasmuch as a stacked beam radar with coherent MTI has not been previously observed. Our assessment of the postulated threat over the next 10 years must be increased because of this demonstrated capability. Furthermore, we may expect to see further deployment of this radar. Finally, the presence of this radar and its associated interceptor squadron can be expected to decrease the interceptor reaction time in the vicinity of A from 30 minutes to 10 minutes.

ESM and RHAW

In the best of all possible worlds we would want every signal intercept to contribute to the total analysis process. But in the real world two factors prevent that–end use and time. These factors are the ones that differentiate ESM and RHAW from ELINT. Let us consider ESM first.

ESM. The tactical commander has limited ECM resources, namely only those operational black boxes which are available and which are compatible with his aircraft. His interest in a new signal is only that he wants his force to avoid threats it cannot cope with. His primary interest is to know where the enemy threats are located and how they are employed. Furthermore, he wants current information on which to base today's mission plan. Thus he does not want the detailed second and third stage outputs and he cannot wait for them either. Consequently, ESM consists primarily of raw data with just enough analysis to establish the identity and location of the signals, and to indicate similarities and differences with previous employments of those signals.

It would be easy to conclude from this that one could simplify the ESM equipment because the data will have only limited and short-term usage. But there are two other considerations which mitigate against this approach. First, ESM requires signal identification, and this difficult task may depend on subtle variations in signal parameters. If less capable equipment is used for ESM in a dense signal environment there is the danger that the equipment is incapable of the necessary discrimination. Sccond, having separate ESM resources means purchasing more total avionics and airframes, and in an era of declining or stablilized budgets, the resulting expense may be unsupportable. Thus ESM will very likely share the same collection platforms as ELINT, and the difference will be seen in operational control, in the amount of analysis performed and in the user. That, is, ESM is likely to be "preliminary analysis output" which goes to the tactical commander while ELINT will be the final analysis output and it will go to the rear echelons.

RHAW. With RHAW the time factor becomes supremely important, for its function is to warn the aircrew of their immediate threat. Thus the analysis capability must be built into the equipment. This, in turn, creates a certain amount of inflexibility since the equipment can only mechanistically compare the existing signal with the known parameter limits. And its output is given to crew members whose goal is to stay alive while performing some other primary task. So they, themselves, have no time for analysis.

The easiest RHAW task is to alert crew members that signals are present; but that is only useful in sparse signal environments, in a dense environment such a warning is trivia. A more difficult task is for the equipment to identify the signals that are present and indicate the degree of threat based on the typical employment of that signal. This information is really the first level of what the crew wants, since crew task priority depends upon the threat to their primary mission.

But signal identification in a (probably) dense environment has all the attendant problems of de-interleaving. In this case, the equipment will probably rely on frequency diversity and signal strength; that is, the most dangerous signal is the strongest, and different signals associated with the same system are probably separated in frequency to avoid interference and the consequent system malfunction. But even so false responses are a persistent worry, due to active enemy attempts to produce such responses, to friendly signals with characteristics similar to enemy signals[13] and to the random signal combinations possible in an uncontrolled environment. The most dangerous aspect of false responses is not the immediate effect on the mission, which may be serious, but rather that excessive false responses will lead the crew to disregard all responses.

The most difficult RHAW task is to determine the direction of the threat, since this implies either multiple antennas to achieve directivity or an analysis capability over a period of time. In either case, the avionics payload of the aircraft must increase. If one only wants gross directional information for threat avoidance, then the increase may be small and tolerable. But if precise directional information is required for threat attack the increase is likely to be substantial.

From this discussion, it is easy to see that while ELINT and ESM equipment may be very expensive because of its technical complexity, RHAW equipment may be equally expensive, both because the mechanized analysis implies sophistication and because the tendency will be to equip every aircraft in the fleet. Conversely, the high cost may drive one to take short cuts which, although they function correctly in sparse environments, may be more likely to malfuntion in dense environments and destroy the credibility of the equipment. One might attempt to remedy this problem by using digital computation, so that the equipment can be missionized through soft-

[13] Because the emphasis of RHAW is on enemy signals, the existence of these friendly signals is easily overlooked until combat deployment inescapably reveals their presence.

ware, but such an approach will undoubtedly increase the basic cost of all equipment, independent of its use.

In summary, we may conclude that while the basic limitations on ELINT are analytical, the basic limitation on ESM will be operational and those on RHAW will be electronic. In addition, both ELINT and RHAW will have budgetary limitations, ELINT, because of the analytical costs in people and computers, and RHAW because of equipment quantity. This does not say that other problems do not exist, but rather they can probably be surmounted given enough ingenuity. In any case, the real challenge of electronic reconnaissance is to obtain a timely, useful and accurate product at a reasonable cost. If we fail in that, then the total house of electronic warfare can collapse.

Chapter 5

ELECTRONIC COUNTERMEASURES

Introduction

The second major division of Electronic Warfare is ECM, and of the three divisions it is probably the best known. Partly, this is a result of the fact that ECM tends to be embodied in "black boxes" which are the visible realization of electronic warfare. Often it appears that if one understands the black boxes then one has an understanding of ECM, but such an attitude is very narrow because it ignores the total problem of the employment of ECM in warfare. Thus our approach in this chapter will be more general; we will attempt to lay down the framework within which the black boxes function.

Although the general principles of ECM apply to the ground, air, and sea forces, we will concentrate on the employment of ECM on aircraft and missiles for the following reason. In the higher frequency bands, commonly used for sensors, the radio horizon is very short for surface-based forces due to line-of-sight transmission. Consequently, much of the complexity of ECM is not seen until one of the two contestants is airborne, so that many land and sea force ECM problems occur when they employ or face airborne weapon systems. Thus we will consider airborne attack because it exhibits all the potential ECM interactions.

Of the two types of electromagnetic radiating systems against which ECM may be employed, sensors or communications systems, the enemy sensors receive by far the most attention for two reasons. First, an active *sensor* operates by transmitting energy and receiving reflected energy. A passive sensor only receives energy. But for both types, if our forces are detectable by an enemy sensor, they are also in a position to employ ECM against it. A *communications* system, on the other hand, is usually located so as to make it as inaccessible to us as possible. Thus the sensor is the more accessible of the two systems to our ECM.

Second, if we deny the enemy the use of a communications system, then we usually prevent ourselves from eavesdropping that system also. Furthermore, denial over a long period of time will cause the enemy to react by building a more inaccessible system which will be more difficult both to deny and to eavesdrop. Consequently, only if the short term advantages are paramount is it desirable to deny the enemy the use of a communication system with ECM. In most cases, the long-term advantages of clandestinely eavesdropping override all other considerations.[1]

Typical electronic sensors against which ECM might be used include long range passive detectors, radar warning picket ships, airborne radar patrols (AWACS), long-range early-warning radar sets, ground controlled intercept radar sets, fighter intercept radar, missiles guided by radar or infrared, radio and radar navigation equipment. electronic bombing equipment, electronic identification equipment (IFF), terrain following radar. anti-aircraft artillery (AAA), fire control radar, surface-to-air missile (SAM) control radar, etc. The particular method of employment will depend upon the tactical situation.

In order to be specific we will select the situation where our aircraft are penetrating an enemy air defense. In that case the sensors are primarily radars of two general types: Those radars whose purpose is to keep a large area under surveillance and those radars whose purpose is to precisely locate a single object. The former task is usually performed by radars of the general type known as *search radars*. These radars may be further broken down into early warning (EW)[2], ground controlled intercept (GCI) and target

[1] A more detailed discussion of this point is covered in Chapter 7.

[2] Careful readers will note that the abbreviation EW has been used for both electronic warfare and early warning. This duplicate use is widespread and the reader must rely on context to indicate the intended use.

acquisition (TA) radars. The latter task is usually performed by radars called *tracking radars*, although optical and/or infrared (IR) sensors may also be employed. Since tracking radars usually exist to provide precise guidance to some weapon system, they are usually identified by the weapon system they control. Radars used for controlling fighter weapons are called airborne intercept (AI) radars, those used to control SAMs are called missile control (MC) radars and those used to control AAA are called fire control (FC) radars.

ECM Concepts

As the result of their experience in World War II, the survivors of those electronic warfare battles concluded that there were five EW concepts that could be used by the attacking force.[3]

1. *Ignore* the defender's electronic sensors and accept any consequent losses.
2. *Avoid* the defense and its sensors.
3. *Dilute* the defense with false information generated either electronically (deception) or with decoys.
4. *Degrade* the operation of the defender's electronic sensors and communications equipments with jamming or deception.
5. *Destroy* or damage the defense sensors and its weapons.

The opinions of the World War II EW pioneers should be treated with great respect. That was the most recent war where major powers were at battle with their immediate existence at stake. Hence the EW battle in World War II was a no-holds-barred, agressive one. Since then, no major power has shown all of its EW secrets. Nevertheless we may have obtained a good look at some Soviet developments during the last Czechoslovakian invasion.[4] Conversely, the communist bloc probably has seen some of ours in Southeast Asia. But even in the lesser conflicts, some lessons are to be learned (or re-learned):

1. Penetrating aircraft need EW warning systems (RHAW or alternative systems) and sufficient active ECM to protect themselves in combat.
2. It is as effective to kill or wound the technically trained personnel operating the defense as to destroy the system itself.
3. There is a sixth tactic that can be successfully employed by an attacking force—*intimidation* of the defense. The threat of death or destruction by an attacking force can greatly reduce the effectiveness of any air defense, for example, by making the radar operators affraid to turn on their radar at critical times.

This last lesson was also learned in World War II when the British flying bomb was effective against German radar crews. Some crews actually abandoned their radar site when the British airplanes came close.

Of these last three lessons learned we have already discussed RHAW in the previous chapter. The idea that destruction applies as much to personnel as to logistics expands the types of weapons that we can use. It is the third lesson which we want to draw attention to. It is all too easy to forget that warfare has a psychological side, especially in this modern age where everything must be quantified. It is clear that intimidation, like deterrence, demands that we demonstrate in some manner our ability to carry out our threats. But having demonstrated that our weapons can be effective in some instances, intimidation allows us to gain additional benefit in suppressing enemy defenses beyond our actual kills. Hence, through intimidation weapons and tactics which statistically are not very effective can yet be very valuable. (Similarly, a football team with a predominantly ground attack may find that an occasional passing attempt is most valuable in that it keeps the defense from setting against their ground attack). Of course, this idea of intimidation can be used by the defense also,

[3] *Electronic Warfare Officer*, USAF Annual Navigator/Observer Academic Refresher Course Student Study Guide. (Mather AFB, Calif: Department of the Air Force, August 1962), pp 3-4; and unpublished text, Electronic Warfare School, Keesler AFB, Mississippi, 1954.

[4] Likewise, such EW activities as the jamming of the Voice of America broadcasts give us some insight into enemy capabilities and concepts.

but we will confine our attention to the penetrators.

These historical concepts are summarized in Table 16, along with the type of ECM and the corresponding tactics that tend to be employed, and the usual reaction of the defense. We shall expand these concepts in more detail in the paragraphs that follow.

In view of the concepts of Chapter 3, we must recognize that there is an interaction between the defense and the use of ECM by the penetrating force. Light defenses mean that the protection of ECM is not worth the loss in weapon payload and range. On the other hand, penetrator success in attacking targets motivates the defense to increase its capability, and then the penetrators find ECM more valuable. Thus one can roughly equate the intensity of the defense to the level of ECM employed, and in turn, one can predict the probable defense counter to the ECM it experiences.

Ignore and Avoid. Only if the defense is very light can the penetrator completely ignore it, since this concept implies that one can fly with impunity anywhere. Usually it applies only to areas where it is believed that there is no defense, and even in that situation the penetrator jinks (makes random changes in heading and altitude) to lessen the success of any unexpected defense.

In general, it is more common to avoid light defenses by detouring around them. This embodies the obvious fact that if we can

Table 16

The Total Spectrum of ECM

Defense Intensity	ECM Concept	ECM Type	ECM Tactics	Defense Reaction to ECM
Light	Ignore	None	Maneuver	None
	Avoid	RHAW	Maneuver	None
Medium	Dilute	Deception[1]	Decoys	ECCM
	Degrade	Jamming Deception[2]	Self-protection[3] Support[4]	ECCM Alternate modes of operation
Heavy	Destroy Intimidate[5]	Homing missiles[6] Bombs	Suppression[7] Hunter-killer[8]	Emission control Dummy defenses Barrage fire

[1] False target generation only.

[2] Primarily gate-stealing techniques (see text).

[3] Self-protection ECM is that carried on-board the weapon carrying penetrators.

[4] Support ECM is all ECM carried on other aircraft and includes both escort and standoff ECM.

[5] Intimidation is a psychological concept that relies on a demonstrated capability to destroy the defenses.

[6] Anti-radiation missiles (ARM), missiles that home on the defense radar sensors.

[7] Suppression is basically intimidating the defense during the time the strike aircraft are delivering their weapons. It does not seek to destroy the defense, only prevent it from firing.

[8] Hunter-killer has as its main objective defense destruction and does not necessarily operate only when weapons are being delivered on targets by strike aircraft.

launch telling blows by side-stepping the defense, then it is in our interest to do so. But the most valuable targets are usually the best defended, so detouring must eventually stop. However, we should not overfly heavy defensive weapons complexes to get to our target if such a route can be avoided. Neither should we repetitively use the same penetration route or the same strike tactics since that is an invitation for the enemy to set up and organize a heavy weapon complex.

Avoidance can use the *information* gathered by ELINT pertaining to enemy radar range and altitude coverage. It may be possible to fly high enough to avoid detection of a radar with poor high-altitude coverage. Or by flying low, the presence of the aircraft may be concealed from a radar set having poor low-altitude coverage. Another means of avoiding detection is to penetrate an area of incomplete radar surveillance. The ability to detour around the defense may be aided by using RHAW equipment to locate the electronic sensors which comprise the eyes of the defensive systems.

Avoidance also encompasses the technique of *radio silence*. Enemy passive detection sites locate approaching aircraft by their electronic transmissions. These transmissions may originate from the aircraft communications equipment, navigational radar or jammers. If electronic emissions from the aircraft are kept to a minimum, detection by the enemy passive detection sites may be avoided.

Dilution and Degradation. These two concepts reduce the defense to the point where we can accomplish our mission with acceptable losses.[5] In these areas ECM becomes very closely allied with tactics and the total effect on the defense depends upon the symbiosis of ECM and tactics. Because the total effect depends upon the interrelationship between ECM and tactics the effectiveness of ECM is often difficult to assess. Consequently, valid data on the effectiveness of ECM in actual combat is scarce. As a result, ECM concepts are usually discussed in simple idealized frameworks to avoid the complexity which obscures what is happening. For this reason we shall also continue our discussion with reference to simplified situations.

Dilution on the one hand, refers to those techniques which are used to make a penetrating force seem larger than it really is. The idea is to make the enemy engage "aircraft" which either do not exist, or which pose no threat to him (decoys). In that way his lethal weapons are diluted, expended uselessly, and the survival of the penetrating force is increased.

We may class the techniques of dilution as either mechanical or electronic, the distinction being based on how the extra "aircraft" are produced. If the dilution is mechanical it means that there are extra physical objects in the air which look like penetrating aircraft. These objects may be small airframes or drones, such as the QUAIL, or they may be clouds of *chaff*, small lightweight strips of aluminum or metallic-coated glass fibers. Electronic dilution, on the other hand, means that there are no extra physical objects, the false targets seen by the radars are generated by deception ECM in the penetrating aircraft. (We will discuss this technique in more detail latter). One might combine these two ideas by having separate disposable jammers as mentioned in Chapter 3. But the overall objective is to add enough apparent aircraft to the airspace that the defense is overwhelmed and cannot sort them out, so that its weapons are expended uselessly. For this reason feints, false penetrations, are classed as examples of dilution.

Degradation, on the other hand, means that our ECM is intended to reduce the electronic efficiency of the defenses' sensors. One way of accomplishing this is to jam: transmit noiselike signals which interfere with the operation of his radars. We may also modify

[5] We might note in passing that it is often an operational fact that the overall tactical aircraft loss rate is an invariant of the mission. That is, the risk of the targets attacked is controlled by the acceptable loss rate. If the loss rate decreases we press on to more risky targets; if it increases we pull back to easier targets.

our aircraft so that they are less detectable. A third technique uses electronic deception[6] to interfere with the proper operation of his equipment through such techniques as gate stealing, inverse conical scan, etc. A fourth technique uses chaff bursts, flares, or expendable jammers to draw off his homing missiles.[7]

Destruction. This is the most positive of the six countermeasure concepts. However, with present technology destruction requires high explosive or nuclear devices. These weapons have only a one-time use, in contrast to most electronic weapons which can be used repetitively.[8] Consequently destruction is usually expensive and used only when the sensor must be denied.[9,10]

Destruction does have one primary advantage over the other tactics, the resulting hole in the enemy's radar coverage exists until the site can be rebuilt or replaced. This tactic also reduces the number of skilled technicians available to the enemy both by direct casualties and by requiring skilled manpower to repair the site.

Destruction, then, would probably be used only on the more important enemy electronic installations such as GCI and acquisition radar sites. The number of enemy radar installations would prohibit this most effective countermeasure from being used to eliminate all enemy radars. Hence the strike commander must trade off the benefit of site destruction against the cost of that destruction.

For example, it is more exciting and viscerally satisfying to destroy missile control sites (terminal threats); but since most SAM sites are mobile, the strike commander must expend a large ESM effort in an attempt to target the mobile sites accurately enough to be certain of destroying them. Furthermore, the defense will probably have more terminal threat sites than any other since they are short range systems. Thus it appears much more effective to attack the surveillance (EW, GCI and acquisition) radar sites for three reasons. First, the requirements of radar netting make moving a surveillance site a time-consuming process, so they will be relatively fixed and hence easy to target. Second, these are "area" sensors and there will be relatively few of them compared to the total number of radar sites. Third, destroying surveillance sites prevents the enemy from organizing his defense and leaves the terminal sites without guidance as to their designated targets; thus they must flail around and hope to find a suitable victim.[11] Thus destruction needs to be wisely applied to achieve maximum effectiveness.

[6] As used here deception is a technical term describing an ECM device which emits energy in pulses.Depending upon its design such a device can produce false targets, hence realizing the concept of dilution, or it can attempt to steal the "gates" of the radar, thus realizing degradation. Some workers in the EW) field also speak of the concept of deception to cover the idea of the feint, but we have chosen to class this under dilution.

[7] One might justifiably argue that this technique is more a concept of deception (see previous footnote)than degradation. One must recognize that all varieties of techniques exist and we have chosen this organization to avoid as much overlap as possible.

[8] The advent of the high power laser may change this by providing us with a reusable destructive weapon.

[9] We do not mean necessarily that bombs or rockets are in themselves more expensive than ECM equipment. Rather destruction requires a high probability of physical damage which requires, in turn, a certain delivery accuracy. Locating even a large radar set precisely is not easy, especially when an enemy is not likely to allow overflight if he can help it. Then one must deliver the bomb to that location. Typically nuclear warheads have relatively large radii of destruction so the delivery accuracy (usually specified by the circular error probable (CEP), the distance from the aim point within which one half of the weapons fall) can be low. Thus the delivery system can be relatively cheap but the logistics and political costs of the warheads themselves are high. On the other hand, conventional warheads have relatively small radii of destruction hence requiring good delivery accuracy, usually much better than the delivery system CEP. Thus one must use large quantities of bombs and the cost, including the sorties that must deliver them, is also high. See Appendix C.

[10] A good example is the attack on the German coastal radars prior to the Normandy invasion in World War II. See Alfred Price, *Instruments of Darkness*, (London: William Kimber, 1967), pp 199-201.

[11] Incidentally, the same considerations apply to achieving air superiority solely by air-to-air combat.

Basic Principles of ECM

Before we turn to the particular techniques used in ECM we need an appreciation of the influence that the objectives, methods and constraints of ECM have on its realization. This appreciation will help put the detailed discussions to follow in perspective. We will begin by considering the operational employment of ECM since it is the ultimate use of ECM which drives all the other aspects.

The Basic Problem of ECM. The basic difficulty in the operational use of ECM arises from the fact that while ECM is designed to disrupt the defense, it is generated at a point remote from the defense sensors and its effectiveness is constrained by the imperfectly known characteristics of the sensors through which it attacks. Thus we can discuss ECM principles under three headings: first, how is the defense disrupted; second, what is the effect of the distance between the ECM transmitter and the defense sensor; and third, how does the penetrator determine if his ECM is successful? This is the outline of the three subsections which immediately follow.

However, there are some other factors which influence the ECM battle which we must discuss. For example, the aircraft being protected need not carry the ECM, it may be carried by other aircraft or it may be inserted into the airspace to operate independently for its lifetime. This leads to a discussion of support ECM and the three types of ECM. Finally, we must realize that ECM is basically a protective measure. This fact has a definite impact on the urgency of ECM development in peacetime and leads to a highly cyclical development pattern. This pattern must be understood if a consistent ECM program is to be established.

Information Rate and Errors. Basically ECM interferes with the operation of the sensors of the air defense system, and through them, with the operation of the system itself. Briefly, ECM attempts to make the defense more uncertain as to the threat it faces.[12] The greater the defense uncertainty, the more effective the ECM. To put this another way, ECM attempts to reduce the information content of the signals the defense recieves with its sensors. There are two ways this can be done. The first is to add random signals in an attempt to reduce the signal-to-noise (S/N) ratio. By Shannon's law this reduces the channel capacity of the system and thus its information rate. This is the approach taken by jamming.

The second approach is to add "signals" to the system leaving the noise level untouched. In this case, the channel capacity of the system remains constant but it is forced to handle a higher information rate, consequently we can expect the error rate to go up. If the information rate can be made larger than the channel capacity, the error rate should increase rapidly. This is often spoken of as forcing the system into data rate saturation. Deceptive ECM takes this latter approach.

In both cases, the objective is to force the air defense system to make mistakes, or errors. Now the errors can be of two kinds. If the defense believes that there is an aircraft present at a point in space when in fact there is not, the error is called a false alarm[13] or β *error.*[14] The opposite error, not seeing an aircraft that is there, is called a *false dismisal,* α *error,*[15] or *missed detection*[16] in the American literature, but the Russians use a term which translates as "passing of

[12] S.A. Vakin and L.N. Shustov, *Osnovy Radioprotivodystviya i Radiotekhnickeskoy Rqzvedki* [Principles of Jamming and Electronic Reconnaissance] (Moscow: Izdatel'stvo "Sovetskoye Radio", 1968), p 2. Page references are to the machine translation FTD-MT-24-115-69 available from Foreign Technology Division, Wright-Patterson Air Force Base, Ohio, for governmental users and from the National Technical Information Service, US Department of Commerce, Springfield, VA, 22151, for non-governmental users.

[13] *Ibid*., p 14.

[14] J.C. Toomay, *Radar Fundamentals for ABRES Project Engineers,* (Norton AFB, California: Space and Missile Systems Organization, July 1969), p 29. However, other authors reverse the meaning of α and β.

[15] *Ibid.*

[16] Merrill I. Skolnik, *Introduction to Radar Systems* (New York: McGraw-Hill Book Company, 1962), p 423.

target".[17] False dismissals seem to receive relatively little emphasis in radar literature because a radar is designed to reliably detect targets and the many echo returns commonly received from an aircraft make detection more likely and false dismissals less likely.[18] However, the false dismissal probability is not zero so that missed detections do occur, especially in the presence of ECM, and they are as damaging to the defense as false alarms.[19]

From the above description it is clear that jamming wants to use signals which are as random or noise-like as possible. Hence, it is common to find the term *noise-jamming* used in the literature, although according to the current JCS definitions the adjective "noise" is not necessary. Conversely, deception wants to use signals which are as similar to the received radar echoes as possible. In general, we make a distinction between *false targets* and *deception* depending upon the type of radar system being deceived, although the basic signal characteristics in either case are the same, because the signal processing required in the deceiver is quite different in the two cases. We shall discuss this in more detail later in this chapter.

Burnthrough and Lookthrough. Typically ECM is generated at some distance from the radar it is affecting. Furthermore, the aircraft under surveillance is moving about in the airspace. Thus the relative strength of the ECM and the radar echo will vary, and this gives rise to burnthrough, the geometrical relationship at which the strength of the radar echo becomes greater than that of the ECM signal. This phenomena occurs for a large number of radar antennas, to see why we must examine the inverse square law of electromagnetic wave propagation. To simplify the geometrical relationships we shall only consider the case where the ECM transmitter is on board the aircraft under surveillance. The more complex cases will be discussed under support ECM.

As you may remember from Chapter 2, the power density of an electromagnetic wave at any point in space is (see (5))

$$S = \frac{P_t G_t}{4\pi R^2} \qquad (13)$$

where

S = power density in watts/m^2
P_t = transmitter power output[20]
G_t = transmitting antenna gain
R = distance from antenna to point in space.

Now S is the energy per second passing through a surface of unit area perpendicular to the direction of travel of the wave. A radar operates on the energy reflected from the aircraft back toward the antenna. To determine how much energy is reflected it is customary to describe the aircraft in terms of its equivalent reflective area. This is called its radar cross section. The energy reflected back toward the radar becomes:

[17] Vakin and Shustov, *Osnovy Radioprotivodystviya*, p 14.

[18] Skolnik, *Introduction to Radar Systems*, pp 30-35, 423-4. Typically radars with automatic detection circuits are designed by specifying a small false alarm probability (less than 10^{-5}) and a probability of detection greater than 90 percent for a single pulse (which is equivalent to a false dismissal probability of less than 10 percent). From these values the required detection threshold (or its equivalent, the signal-to-noise ratio) can be determined. Then the effect of multiple echo returns from an aircraft (called integration) and other signal processing is added. If the threshold is changed to compensate for these effects, then the false alarm and false dismissal probabilities are unchanged; if the threshold is unchanged, then the false dismissal probability changes. For a typical radar which uses 10 to 15 consecutive echo pulses from a target, the false dismissal probability can become as small as the false alarm probability if the threshold is not changed.

[19] Generally an increased false dismissal probability reduces the detection range of an aircraft. But with certain receivers (CFAR, see chapter 6), and antennas (cosecant-squared, this chapter) a high false dismissal probability in the presence of jamming may cause the aircraft echo never to be detected.

[20] Since the radar emits energy in pulses it is customary to consider the rate of energy emission during the pulse as the power level of the transmitter. This power level is termed *peak power*.

$$P_r = \frac{P_t G_t \sigma}{4\pi R^2} \qquad (14)$$

where

P_r = the reflected radar energy
σ = radar-cross section

If the ECM signal originates at the aircraft then it must travel the exact same path to the radar receiver that the aircraft echo does. Hence it it is to be stronger than the echo at the receiver it must also be stronger when they both leave the aircraft. Typically, ECM transmitters radiate a constant amount of power, but as the aircraft approaches the radar the strength of the radar echo increases because the range is decreasing. Since ground radar transmitters are more powerful than airborne ECM transmitters, there is a range at which the radar echo becomes equal in strength to the ECM signal (Figure 30). That range is the burnthrough range.[21]

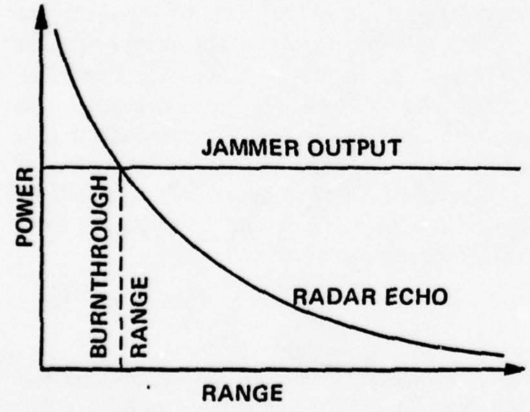


FIGURE 30. BURNTHROUGH RANGE

Usually the burnthrough range is calculated for a standard set of conditons and used to compare the effectiveness of ECM against various radars. But it should be understood that, in practice, the burnthrough range is never a constant. First, the reflective properties of the aircraft can vary over a range of 1000:1 depending upon the particular aspect presented to the radar. Second, the ability of the radar to distinguish its echo from the ECM depends on its design, its condition of maintenance, and on the signal processing circuits in use at the time. That is, burnthrough to the operator or automatic detection circuit may occur when the echo is either stronger or weaker than the ECM signal depending upon the radar configuration and condition.

A third factor in burnthrough range is the radar antenna pattern. The idea of a radar self-screening range implies that as the airplane approaches the radar the radar antenna gain is constant. For a tracking radar where the antenna will always be centered on the airplane this assumption is valid. But for a search radar this assumption implies that the airplane descends as it approaches the radar, since the radar antenna pattern is usually fixed in elevation. In a normal situation, however, the airplane will fly at a constant altitude when approaching the radar (Figure

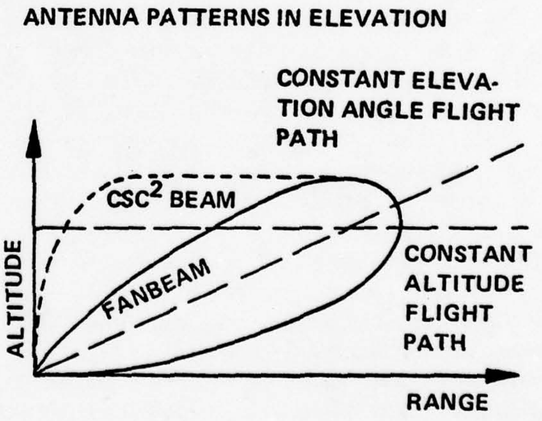

ANTENNA PATTERNS IN ELEVATION
CONSTANT ELEVATION ANGLE FLIGHT PATH
CSC^2 BEAM
FANBEAM
CONSTANT ALTITUDE FLIGHT PATH
ALTITUDE
RANGE

FIGURE 31. RADAR ANTENNA PATTERNS WITH AIRCRAFT FLIGHT PATHS

[21] Burnthrough range is usually used by radar operators who want to see the aircraft through the jamming, *Self-screening range* is usually used by jammer designers and airborne EWOs (electronic warfare operators) who want to hide their jamming. Self-screening range is not usually applied to deception although the concept is applicable.

31), so that the elevation angle of the airplane, and consequently G_t, will change. Nevertheless, for many radars–especially those called fan-beam radars–a self-screening range does exist. But for some radars (especially those of the cosecant squared–CSC^2–antenna pattern type) a self-screening range does not exist. For these latter radars if the echo is less than the ECM signal at maximum range it will always be less.

The final factor affecting burnthrough range is the ECM antenna pattern. Because ECM transmitters are limited in power it is common practice to give the ECM antenna some directivity to increase the ECM effectiveness. But if the aircraft attitude changes the ECM antenna will tilt and the power directed at the radar will change, unless the antenna and/or its pattern is stabilized, an expensive feature. Even without considering directivity, the ECM antenna pattern is very likely irregular because the antenna is mounted on an irregular surface–the aircraft skin. Hence random changes in the ECM power are to be expected.

The effect of these four factors is that the ratio of the ECM power directed at the radar to the radar echo power (the so-called jamming-to-signal or *J/S ratio*) will continually change. Thus the burnthrough range is a dynamic quantity depending upon the instantaneous conditions of the battle. Yet it continues to be used because there seems to be no other representative quantity which can be used to compare different ECM techniques.

The other basic principle related to aircraft/radar geometry is lookthrough. The concept of radar cross section implies that we
4 can consider an aircraft as an equivalent metal sheet perpendicular to the aircraft-radar line-of-sight which reflects radar energy. Aircraft radar cross-sections typically range between one and one thousand square meters. Now in order to use its ECM effectively the aircraft must also have a receiver with an antenna so that it can determine when to employ ECM. The receiver antenna effective area is typically quite small, on the order of 0.01 square meters, so as to not interfere substantially with the aircraft aerodynamics. Thus the receiver must sense a very small portion of the energy reflected from the aircraft.

What happens when the ECM transmitter is turned on? It radiates more power than the aircraft reflects and it is located very close to the receiver antenna. Unless suitable precautions are taken all the receiver will hear is its own ECM transmitter, it becomes blind to all other signals.[22] The radar being countered could stop transmitting, or change frequency, and the aircrew would not know it. Therefore the operator needs to "look through" his own ECM so that he can continue to assess the hostile radar environment.

An even more dangerous situation occurs if the ECM equipment is designed to operate automatically in response to a radar signal. Then the lack of lookthrough can cause the ECM to respond to its own transmissions. In that situation, once the ECM responds to one signal it will never turn itself off; the ECM transmitter becomes a beacon broadcasting the aircraft location to anyone who will listen.

One solution to the problem of lookthrough is to isolate the receiver and the ECM transmitter. The amount of isolation needed is at least the ratio of the aircraft radar cross-section to the effective area of the receiver antenna times the ratio of ECM power to radar echo power at maximum range from the radar. From the figures presented previously it is apparent that the required isolation is rarely less than 100:1 in power (20 dB) and can range as high as 100,000:1 (50 dB) or more. Because of the close proximity of the receiving and transmitting antennas such isolation is often difficult to achieve.

The only other solution to lookthrough is to turn the ECM transmitter off periodically to allow the receiver to look for the radar signal. Of course, the ECM protection may be lost when the transmitter is off unless the

[22] Note that lack of lookthrough is much more serious with continuous ECM (jamming) than with pulse type ECM (deception). Nevertheless, without proper design attention a deceiver can blind itself also.

AD-A065 453 AIR FORCE ACADEMY COLO F/G 17/4
THE STRATEGY OF ELECTROMAGNETIC CONFLICT,(U)
FEB 79 R E FITTS

UNCLASSIFIED NL

2 OF 3
AD
A065453

turn-off time is very short. Hence, if lookthrough can be done quickly enough there may be no perceptible decrease in the burnthrough range.

Indicators of Effective ECM. Now let us turn to the third problem, how does the ECM operator know if he is being effective? In general, if his ECM technique involves radiating energy he can tell if the transmitter is operating properly. But that measurement is conducted at the aircraft, not at the radar against which the ECM is being employed. Consequently, he wants most some further indication of effectiveness, but this depends very greatly upon the radar *system* he is attacking. So let us look at these systems in greater detail.

It is customary to classify radars as either *search* or *tracking* radars depending upon their design. A search radar surveys a large volume of space to determine what aircraft are present; a tracking radar looks at just one aircraft to determine the precise position and velocity or track. However, the ability of an ECM operator to determine whether his efforts are effective does not depend upon the radar type but upon the system which uses the radar. To describe the system we will use two different terms: *mono-track* and *track-while-scan* (TWS). The distinction is the following. A mono-track system follows only one aircraft at a time, the TWS system can follow several. Typically, a mono-track system uses a tracking radar such as a conical scan or monopulse radar to align the axis of the antenna mount with the aircraft. Then the system measures the azimuth and elevation angles of the mount, and combines that information with the radar range to determine aircraft position. By following the change in position over a period of time, the system can measure velocity and track.

The two important features of the mono-track system are that (1) it can only follow one aircraft at a time, and (2) the antenna must be pointed at the aircraft for the system to work. ECM can deny range to the radar, but the antenna can still seek out the direction of the received ECM and thus determine the direction of the aircraft. But deception, specifically certain inverse gain techniques, has the capability of causing the antenna not to point at the aircraft. At this point, not only is the defense getting false information, but the aircraft knows it because it can sense that the antenna is pointing somewhere else. Thus in this instance, the ECM operator has a direct measure of his effectiveness.

Now let us consider the track-while-scan system. Here the system is prepared to track more than one aircraft. It does so by looking at the aircraft in sequence, that is, by covering the total volume of interest and noting where it sees aircraft. For each aircraft detected it remembers its position and compares that with the position it finds on the next look. After two or three looks, it is not only able to tell the position of each aircraft but it has a fairly accurate track. In this system, some sort of a memory–and by implication, a computer–is required. Furthermore, since the system only occasionally looks at each aircraft, its track information is not as accurate as in the mono-track, where the aircraft is under continuous observation. Hence, if the aircraft track changes suddenly or rapidly, the system can lose the aircraft, a false dismissal error.

The most important aspect to the ECM operator is the fact that since the system only observes his aircraft occasionally, it gives no indication whether it is tracking him or not. Thus he has absolutely no direct indication as to whether ECM is effective. Modern phased-array antennas are almost always used in a TWS system[23] and the conventional EW/GCI radar net is very close to such a system. The only way in which the EW/GCI radar net commonly deviates from a true TWS system is that special radars, called *height-finders*, are used to determine aircraft height

[23] Tomay, *Radar Fundamentals*, p 31, comments that some phased array radars can both track and search simultaneously. This is called "Track and Scan". The indications received by the ECM operator in such a case might be either mono-track or TWS depending on whether the tracking was done by changing the scan pattern or by multiple beams.

because the conventional search radar cannot do so. Hence, an aircraft illuminated by a height-finder knows that he is being tracked. But the disappearance of the height-finder does not indicate loss of track because height-finders customarily move from aircraft to aircraft in order to obtain height for the total raid.[24]

To summarize, only in the case of the mono-track system does the ECM operator have any indication as to whether his efforts are effective. Since mono-track systems usually provide terminal guidance for weapons, such information is more than welcome. But TWS systems provide no such indication, so that the ECM operator is ignorant of the success or failure of the radar operator. For this reason ECM has long been considered a kind of "black art" by many crewmen and commanders.

On-Board and Support ECM. Up to this point we have considered that the ECM originates on-board the aircraft being protected. This is not necessarily so, and such a situation modifies our comments somewhat. *Support* ECM, ECM which originates on some other vehicle, still has a burnthrough or *screening range*, because the ECM output is constant while the radar echo increases in strength as the aircraft approaches the radar. However in this case, the path, traveled by the ECM signal and the radar echo to the radar antenna are different, so there is another factor to be considered. This factor is most important when the radar is pointed at the protected aircraft and not at the ECM aircraft. In this situation the radar is much more sensitive to the echo than to the ECM and tends to discriminate against the ECM because of the radar antenna pattern. This situation is commonly called *sidelobe jamming* (although it applies to deception also) and is the reason that support ECM commonly requires much more power than self-protection (on-board) ECM.

In some cases, a commander may attempt to avoid the problems of sidelobe jamming by sending the support aircraft along with the strike aircraft being protected. This tactic is called *escort jamming* and is contrasted with the situation where the ECM aircraft does not accompany the strike aircraft, called *stand-off jamming*. (Both terms are used for deception also.) Escort jamming gives more ECM protection to the strike aircraft but it does so at a greater risk to the support aircraft. For if it can, the defense will preferentially attack the ECM aircraft in order to deprive the remainder of the strike of its protection. Support ECM thus has several hindrances but it may be used none the less because it gives the commander more options in tactics.

Of course, the ECM support aircraft has its own lookthrough problems, but the distance between the support aircraft and the protected aircraft is typically large enough (unless they are flying in formation) that the support ECM transmitter does not blind the receivers of the protected aircraft. This is especially important since it allows RHAW equipment to function in spite of the support ECM.

The Three Classes of ECM. Given that we want to interfere with an enemy air defense system by inhibiting its sensors, how may we go about it? In general there are three methods and each designates a class of ECM.[25]

1. Radiate active signals to interfere with the radars.
2. Change the electrical properties of the medium (the atmosphere) between the aircraft and the radars.
3. Change the reflective properties of the aircraft itself.

The first class encompasses most jamming and deception. The second includes such techniques as chaff and absorbing aerosols.[26] The third class includes radar absorbing materials (RAM) applied to the aircraft and, conversely, both electronic and

[24] If the search radars should be rendered ineffective due to ECM, then a height-finder may be used as a tracking radar because of its typically greater resistance to ECM. In this event, the height-finder becomes part of a mono-track system but the aircrew can only infer this from the fact that the characteristic height-finder signal does not disappear.

[25] Vakin and Shustov, *Osnovy Radioprotivodystviya*, p 1.

[26] Armand L. Dilpare, "Chaff Primer", *Microwaves* 9 (December 1970): 46.

mechanical echo enhancers for decoys. Table 17 summarizes these techniques, and other techniques to be discussed later, in terms of these three classes and the JCS definitions. Since these techniques will be discussed in more detail in later sections, we shall not spend more time on these principles now.

Table 17

ECM Techniques by Class and Type

	TYPE (JCS MOP 95)	
Class	Jamming	Deception
1. Active Radiators	Spot Jamming Barrage Jamming Sweep Jamming	False Target Generators Track Breakers
2. Medium Modifiers	Chaff Corridors Absorbing Aerosols	Random Chaff Chaff Bursts
Reflectivity Modifiers	Vehicle Design RAM	Vehicle Design RAM Echo Enhancers Corner Reflectors

The Defensive Nature of ECM. Finally we ist consider the fact that ECM is primarily a tective measure, a defensive technique. us the basic measure of effectiveness of M is a negative one—the defense does not ck. Because it is very difficult to measure non-attack of the defense, the ECM user n has no real assurance that he is being ctive. Even though combat statistics seem ndicate that ECM is being effective the ical commander and the aircrews have direct feedback to assure them that they loing the right things.

is problem is primarily psychological, it o direct impact on whether ECM works particular situation. Yet, on the other . it can have a great influence on ECM opment, that is, whether the tactical commander has the ECM "black boxes" he needs when he needs them. For the lack of direct feedback of effectiveness means that the commander is likely reluctant to order and to use ECM. Only when the tactical situation becomes desperate is he willing to sacrifice payload for ECM. Consequently ECM is requested reactively, and when it is wanted it is wanted immediately, not after the formal development cycle has run its course. For this reason if ECM development, procurement and training is not emphasized in peacetime, it may not be available when it is needed.

Jamming

Now let us turn to a more detailed discussion of jamming. Table 9 in Chapter 3 noted that a distinguishing characteristic of jamming was that its signal was dissimilar to the radar signal. And the previous section made the comment that jamming used random noise-like signals. What do these characteristics mean?

The Effects of Jamming. Let us approach this problem by considering the signals at the input to the radar receiver. We pick this point to compare them because even though the jamming is generated at the airplane, it is in the radar receiver that the effectiveness of the jamming is determined. Now the jamming signal may not be amplified noise—other waveforms may be more effective—but noise is a basic jamming signal whose characteristics are well known. On the other hand the radar echo is a periodic sequence of pulses. In Figure 32 we show the radar echo first and then the echo with the jamming superimposed. The objective is to conceal the echo. As Figure 32 shows, this means that the average amplitude of the noise must be at least as great as the maximum amplitude of the radar echo to be concealed. This idea can be alternatively expressed by saying that the average power of the jammer must have the same effect as the peak power of the radar echo, or by saying that the *J/S ratio* must be at least unity (zero dB or greater).

This idea needs to be enlarged upon. If the amplitudes of the radar echo and the jamming add linearly in the radar receiver it is

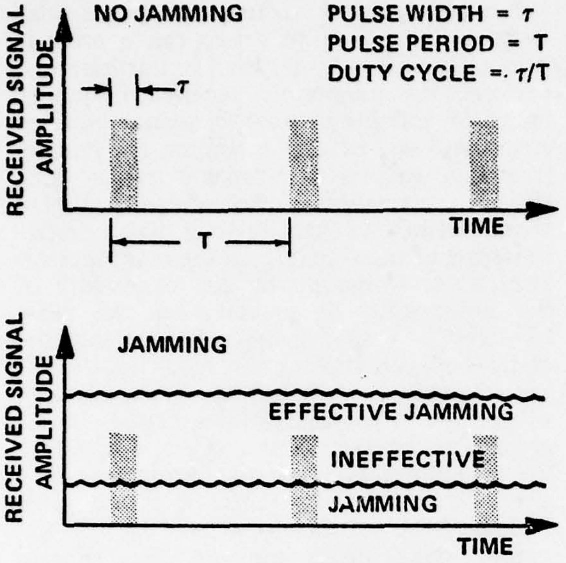


FIGURE 32. RADAR SIGNALS WITH AND WITHOUT JAMMING

theoretically possible to detect a pulse at a J/S ratio of zero dB. However, if the radar reciever has significant nonlinearities–either by design or maladjustment–or if the operator is not well trained, then J/S ratios considerably less than unity may be sufficient to conceal the echo. Thus the susceptibility of a radar to jamming (having its echoes concealed) depends upon many factors. For our own radars it is possible to run tests to determine the J/S ratios required for jamming, for enemy radars we can only estimate from our own experience.

Since the jammer must put out energy continuously while the radar puts out energy in pulses, the jammer pays the penalty of large average power. This in turn requires a corresponding size, weight and primary power supply, all of which must be carried on the airplane. Thus an airplane might be limited in the amount of jammer protection it can carry.

Finally, when the radar antenna is pointed toward the jammer the radar sees signals at all ranges. The effect on a PPI scope is to create a solid line at the azimuth of the jammer. This line, called a *strobe*, indicates to the operator both that a jammer is present and his azimuth; but he does not know the range of the jammer if the jamming is effective. Thus jamming has the bad effect that it can highlight the aircraft's presence and direction and serve to identify it as hostile, but it has the good effect of denying the radar operator the range of the airplane if sufficient power is used. Figure 33 illustrates the idea of a strobe. The left strobe shows the consequence of insufficient jamming power, the aircraft return can be seen "burning through."

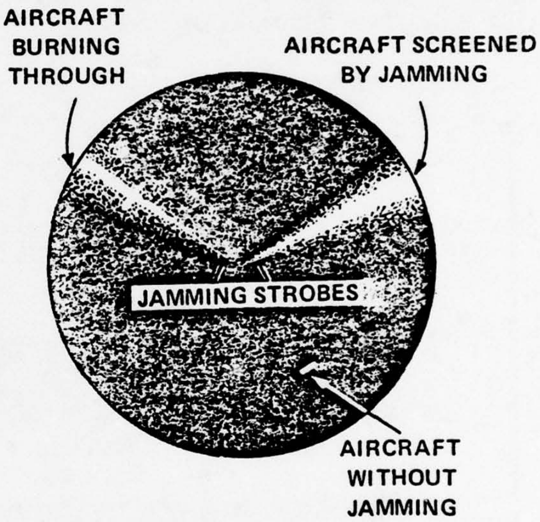


FIGURE 33. RADAR PPI SCOPE WITH JAMMING

The Major Jamming Techniques. Within the general class of jamming there are three different techniques for generating the noise-like signal to be used. In *spot jamming* all the power output of the jammer is concentrated in a very narrow bandwidth, ideally identical to that of the radar. *Barrage* and *sweep jamming* spread their energy over a bandwidth much wider than that of the radar signal. Thus spot jamming is usually directed against a specific radar and requires a panoramic[27] receiver to match the jamming signal to the radar signal.

[27] A special receiver which displays the frequencies of the signals received. See Appendix B for a more detailed description.

The other two techniques however, can be used against any number of radars and only require a receiver to tell them that there is a radar present.

The difference between barrage and sweep jamming lies in the modulation techniques and size of the frequency band covered. *Barrage jamming* often uses an amplitude-modulated signal covering a 10 percent frequency band (bandwidth equal to 10 percent of the center frequency). *Sweep jamming* often uses a frequency-modulated signal and the frequency is swept back and forth over a very wide banwidth, sometimes as much as an octave (a 2:1 band). Figure 34 illustrates these 3 types of jamming.[28]

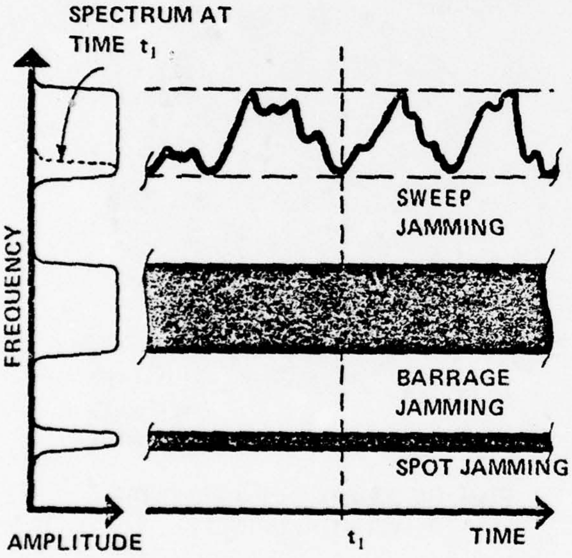


FIGURE 34. SPOT, BARRAGE, AND SWEEP JAMMING

In combat one would expect that spot jamming would be used only when there is an electronic warfare officer in the airplane to tune the jammer. Even in that case it is probably impossible to obtain an exact match between the radar bandwidth and the jammer bandwidth, because of the uncertainty of the frequency of the radar to be jammed. All radars are designed to be tuned over a small frequency band so that two can operate in proximity without interference. Furthermore, because the panoramic receiver frequency indicator and the jammer frequency controls are not exact, exactly matching the jammer frequency to that of a radar is usually done visually on a panoramic receiver. The display characteristics are usually such that a precise centering of the jamming on the radar signal is impossible. Consequently the bandwidth of the noise must be greater than the radar bandwidth. A spot jammer implies that the match between jammer and radar frequencies can be made as precisely as the equipment will allow. A barrage jammer implies that a precise match is not even attempted, rather the jammer covers all the frequencies in a given band. Thus it jams all radars with frequencies in that band.

But this broadening of the jammer bandwidth implies that the jammer requires more power than one that is exactly matched, because the power that matters for any radar is the power that is accepted by the receiver. This fact is usually accounted for by specifying the *spectral power density* that a jammer must have to jam a radar. Power density is the power contained in the jammer output spectrum divided by the bandwidth. Figure 35 illustrates this idea by showing that a jammer of a given total power is more effective if its bandwidth is decreased. The

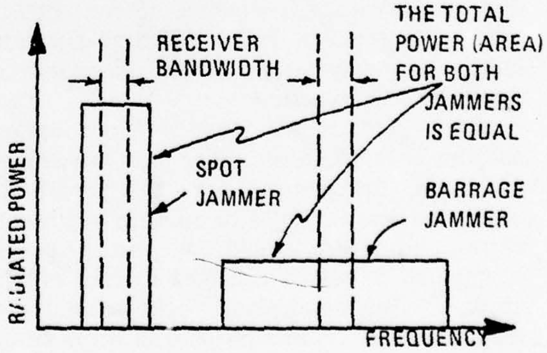


FIGURE 35. RECEIVER BANDWIDTH AND JAMMER SPECTRAL POWER DENSITY

[28] Although it is in general true that the bandwidth of sweep jamming is wider than that of barrage jamming which is, in turn, wider than spot jamming, it is impossible to establish precise limits, since the relative bandwidths are often determined by hardware. The values given in the text are representative.

usual means of sepcifying jammer power density is in *watts per Megahertz (w/MHz)*.

Since aircraft are limited in the total amount of jammer power they can carry, it is advantageous for the air defense network to use as many widely different frequencies for its radars as possible. This concept is usually called *frequency diversity*, and it forces the jamming penetrators to either carry a large number of spot jammers or spread their barrage and sweep jammer power in order to cover all the radars. The ability of a single radar to change frequency to counter a spot jammer is called *frequency agility*.[29]

Deception

The other major type of active (radiating) ECM is deception. In contrast to jamming, deception tries to mimic the radar echo in such a way that the radar will think that it is seeing an echo from another aircraft with a different position or velocity. We can draw a picture similar to that of Figure 32 to illustrate typical deception signals (Figure 36).

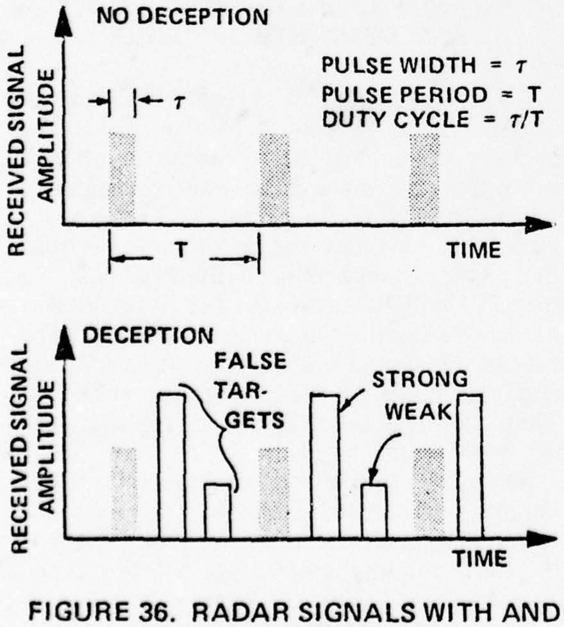


FIGURE 36. RADAR SIGNALS WITH AND WITHOUT DECEPTION

Against any radar, deception has a power advantage over jamming because it emits its energy in pulses similar to the radar pulses (Figure 36). It's advantage is equal to the *duty cycle* of the radar, i.e., the ratio of the average radar power to the peak radar power.

$$P_{av} = P_t d = \frac{P_t \tau}{T} = P_t \tau f \qquad (15)$$

where

P_{av} = average transmitter power
P_t = peak transmitter power
T = pulse repetition period
f = $1/T$ = pulse repetition frequency (PRF)
d = τ/T = duty cycle.

However, this power advantage is paid for, so to speak, by the fact that the false return has a well-defined azimuth and range. Thus the only uncertainty introduced into the defense is whether a particular return represents a target, but it is often a difficult and time consuming task to resolve this uncertainty.

Deceptive ECM, or *deceivers* are called by several names. To avoid confusion we will classify deceivers into two general types: *False-target generators* and *track breakers*. Both types may be realized by transponders (types of *radar beacons*) and *repeaters.* The difference between the two types consists in the type of radars they operate against, so we shall examine them in more detail.

False-Target Generators. False-target generators are typically employed against TWS radars such as search radars with continuously rotating antennas. Their principle purpose is to add apparent aircraft (false targets) into the system, both to saturate the system by giving it too many objects to track and to cause it to overlook the true aircraft. To do so the generator relies on the completely regular scan pattern of the radar to allow it to emit pulses in a pattern that the radar will interpret as an aircraft. The fundamental limitations on the false-target generating technique are the relative difficulty of locating the targets at various places in the

[29] Frequency diversity and frequency agility are discussed in greater detail in Chapter 6.

radar search volume and the credibility of the false-targets generated.

The relative difficulty of locating false-targets at various places in the radar search volume is governed by three quantities: The received radar signal level at the aircraft, the required deceiver transmitter power and the time delay required between the reception of the radar pulse and the emission of the deceiver pulse. Let us illustrate these dependencies by considering the difficulties of generating a false target on a search radar with continuously rotating antenna.

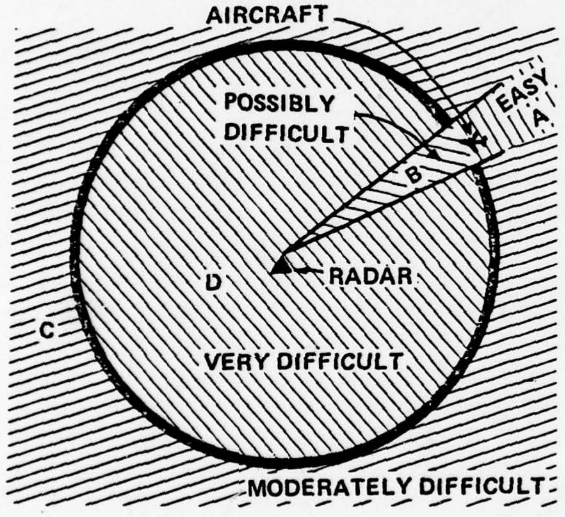
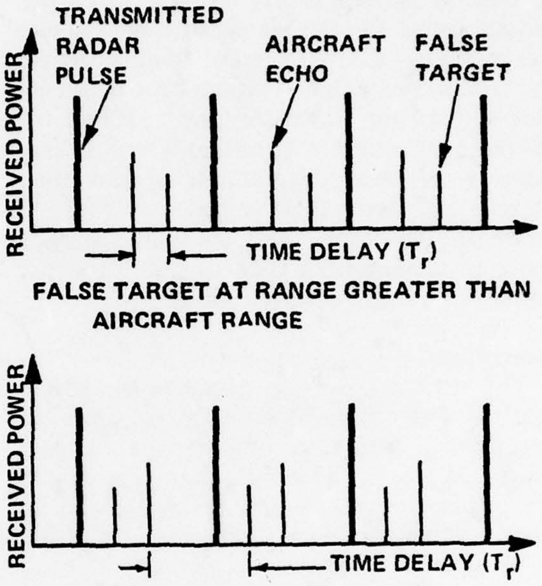


FIGURE 37. FALSE TARGET GENERATION DIFFICULTY FOR A TYPICAL SEARCH RADAR

Figure 37 divides the search volume of our radar into four areas and indicates the relative difficulty of false target generation in each area. The time delay mentioned above governs the ability of the deceiver to vary the range of the false target as illustrated in Figure 38. Specifically, it is clear that for false targets at ranges greater than that of the aircraft (areas A and C of Figure 37) the deceiver pulse must arrive at the radar receiver after the aircraft radar echo. Thus this signal can be generated by transmitting a pulse a fixed time after the aircraft receives the radar pulse. For the false target to be realistic the time delay must be constant, but stable time delays are easy to build.



FALSE TARGET AT RANGE GREATER THAN AIRCRAFT RANGE

FALSE TARGET AT RANGE LESS THAN AIRCRAFT RANGE

FIGURE 38. FALSE TARGET GENERATION AS A FUNCTION OF RANGE

To put a false target at ranges less than the aircraft (areas B and D of Figure 37) the deceiver pulse must arrive before the aircraft echo. Because there is no way to anticipate the radar pulse at the aircraft the false target pulse must be generated by a time delay from the previous radar pulse. If the PRF is stable then T_r will be constant. But if the PRF is not constant, either by intent or through poor transmitter design, either T_r must vary or the apparent range of the false target will vary. Thus putting a false target close to the radar can be difficult.

The major problem in placing a false target in areas C and D of Figure 37 (off-azimuth) as opposed to areas A and B (on-azimuth) is that the radar antenna is no longer pointing at the aircraft. Let Figure 39 represent a search radar antenna pattern. Since signals received by a radar are portrayed as being at the azimuth of the antenna main lobe, false targets in areas C and D of Figure 39 must be emitted when the radar antenna is pointed away from the deceiving aircraft. Thus the signal which the deceiver needs to synchronize its transmitter pulse (i.e. start its time delay) will be weak, and may even be too small to be detected. Furthermore, the deceiver pulse must travel to the receiver through the radar antenna sidelobes (where the gain is less) so that much more transmitter power is needed.[30] Consequently, placing a false target at azimuths away from that of the deceiving aircraft is under the double curse of weak radar signal and large deceiver power.

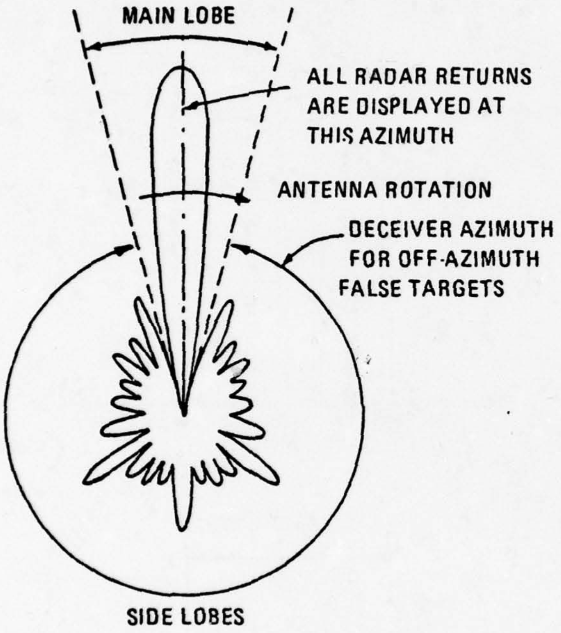

MAIN LOBE
ALL RADAR RETURNS ARE DISPLAYED AT THIS AZIMUTH
ANTENNA ROTATION
DECEIVER AZIMUTH FOR OFF-AZIMUTH FALSE TARGETS
SIDE LOBES

FIGURE 39. A REPRESENTATIVE SEARCH RADAR ANTENNA PATTERN IN AZIMUTH

The limitation of false-target credibility arises from the requirement that the false target should be like an aircraft return–it should have the same breadth, depth and intensity. Intensity is a function of deceiver power and the correct power can theoretically be inferred from the radar signal received at the aircraft.[31] The depth of the blip is proportional to the deceiver pulse width, and it is a relatively easy job to match the width of received radar pulse. However, the breadth of the blip depends on the radar antenna pattern, and that poses a further problem.

Suppose the deceiver transmits a constant amplitude pulse. In this case, it is identical in principle to a radar beacon such as IFF. When the deceiver receives a radar pulse greater than a certain amplitude–the deceiver *threshold* (Figure 40)–it begins to transmit pulses and this continues until the received signal falls below that amplitude. At the radar receiver the amplitude of both the deceiver pulses and the radar echo is modified by the radar antenna pattern. However, the strength of the aircraft radar echo is not constant as the radar antenna sweeps past the aircraft so that the radar echo changes amplitude faster than the deceiver pulse.

This difference in the rate of variation shows up at the radar receiver as an increase in the breadth of the false target over the aircraft return. To this is added any breadth increase due to the deceiver being stronger than the radar echo (Figure 40, right hand illustration). It is the common experience of FAA traffic controllers that IFF returns can be four to six times as broad as aircraft returns, and this provides an easy means of discrimination.[32] Thus to make false targets credible, something must be done

[30] If it is possible to receive the radar side or back lobes and if the maximum jammer power output exceeds the main beam echo from the target by 30 to 40 dB or so, then realistic false targets may be produced on some side and back lobes of many radars by direct amplification and delay of the received radar pulse (that is by a repeater). Transponder operation using the receiver to trigger a transmitter, can ease the requirement for high gain in a repeater.

[31] That is, the variation in the bearing of the radar can be used to determine range to the radar and then the reveived power will allow determination of radar transmitter power. This is the same problem as determining radar location and power in reconnaissance (see chapter 4) and probably requires an on-board computer. However, the amount of computation required to gain a good intensity match is undoubtedly so great as to preclude its being feasible in most situations.

[32] Personal conversations with FAA Controllers.

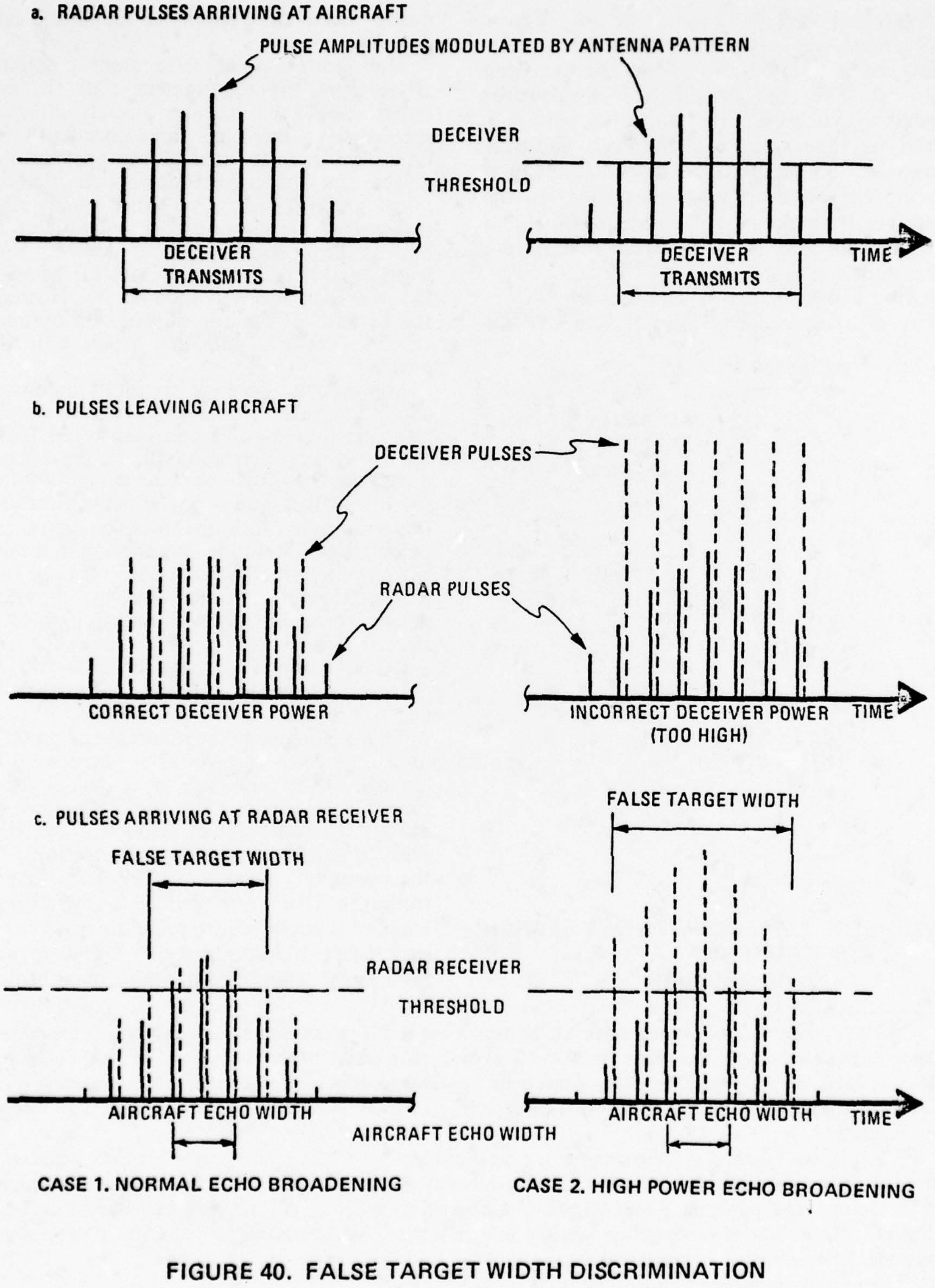

a. RADAR PULSES ARRIVING AT AIRCRAFT
PULSE AMPLITUDES MODULATED BY ANTENNA PATTERN
DECEIVER
THRESHOLD
DECEIVER TRANSMITS
DECEIVER TRANSMITS
TIME
b. PULSES LEAVING AIRCRAFT
DECEIVER PULSES
RADAR PULSES
CORRECT DECEIVER POWER
INCORRECT DECEIVER POWER (TOO HIGH)
TIME
c. PULSES ARRIVING AT RADAR RECEIVER
FALSE TARGET WIDTH
FALSE TARGET WIDTH
RADAR RECEIVER
THRESHOLD
AIRCRAFT ECHO WIDTH
AIRCRAFT ECHO WIDTH
AIRCRAFT ECHO WIDTH
TIME
CASE 1. NORMAL ECHO BROADENING
CASE 2. HIGH POWER ECHO BROADENING

FIGURE 40. FALSE TARGET WIDTH DISCRIMINATION

to make their breadth the same as that of the aircraft.

There are three general approaches to solve this problem. One is to arbitrarily turn the deceiver off so that the false target is the correct width. This technique requires some knowledge of the radar antenna pattern. Another is to vary the deceiver output power in proportion to the received radar signal strength. The third is to put a similar deceivers on board all aircraft to make their radar returns broader. Such augmentation, of course, insures that the aircraft will definitely be seen by the radar.

The result of all these problems is that pure false target generation techniques are not too practical. The situation is somewhat different for track breakers.

Track Breakers. The track breaking deceiver is typically applied against tracking radars associated with specific terminal threats. Because of its association with specific terminal threats it is usually designed for the one-on-one tactical situation and it relies on specific technical parameters of the radar. For that reason there are two generic types of track-breakers–*gate stealers* and *inverse modulation*–depending upon the basic design of the tracking radar. In all cases, however, the basic mechanism involves returning to the radar a *cover pulse*, a pulse much stronger than the aircraft radar echo. The difference between the two types is seen in the behavior of the cover pulse. To understand the reason for this difference let us look in more detail at tracking radars.

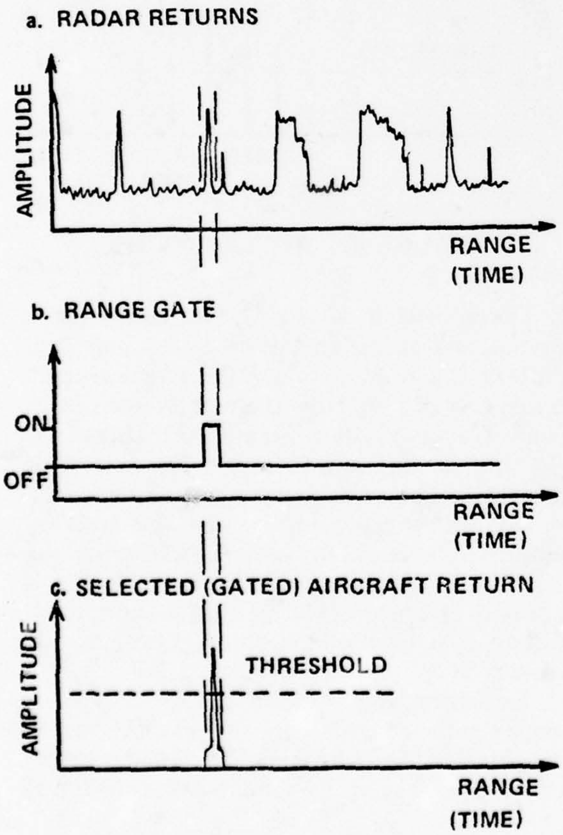


FIGURE 41. RANGE GATING

The purpose of the tracking radar associated with a terminal threat is to determine the target aircraft position and velocity so that the weapon may be guided. For most efficient guidance the weapon should be guided directly to its future impact point, but this requires a prediction of the future position of the target given its present position. The prediction program, or "prediction loop", invariably amplifies the effect of tracking errors–the difference between actual aircraft position and velocity and the measured position and velocity. For this reason most terminal threats use automatic tracking as their preferential mode to minimize tracking errors resulting in maximum accuracy (or minimum miss distance). Conversely the object of a track breaker is to maximize tracking errors and if possible prevent tracking completely.

Whether or not the system controls multiple weapons against multiple aircraft the tracking process by its nature is concerned with a single target aircraft. (That is, tracking two aircraft requires two complete tracking systems however realized). Thus the tracking circuit must select a single aircraft radar echo and follow it, ignoring all other returns (echos). This concentration on a single return is normally achieved by gate circuits in pulse radars, which are nothing more than electronic switches.

The most common gate circuit is the range gate, a switch which is turned on for a short period of time beginning at a certain range (time delay after the transmitted pulse). As Figure 41 shows, if this gate is centered around the radar return the tracking circuit can concentrate on the radar return of interest and exclude all returns and noise at other ranges. In addition, if a radar threshold level is established the exact position of the pulse can be detected without interference from signals at other ranges.

In practice, the range tracking loop endeavors to keep the range gate centered on the selected return.[33] The threshold is typically set using an automatic gain control (AGC) circuit, operating on only the portion of the signal within the gate, whose purpose is to prevent circuit overload on strong signals and excessive false alarms on weak signals. The target range is then taken as the center of the range gate. Thus accurate tracking of the aircraft return by the range gate is essential.

In an FM-CW radar, range is determined by frequency difference between transmitted and received signals at the moment of reception. Thus the "range gate" becomes a narrow filter centered on this difference frequency whose behavior is identical to the pulse radar gate. We shall not discuss FM-CW tracking radars further; however, trackbreaking ECM can be developed against them in direct analogy to that against pulse radars.

Having selected the target aircraft in range, the radar must also track in azimuth and elevation. The method of angle track depends upon the system, TWS or mono-track. In the TWS system the antenna scans systematically past the target aircraft, but the center of the scan pattern need not be pointed at the target; that is, the tracking is done electronically. The range-gated return will vary as the antenna pattern when the antenna scans past the target. Thus we can place an angle gate around that much slower return variation and track in angle in the same manner as a range gate (Figure 42).

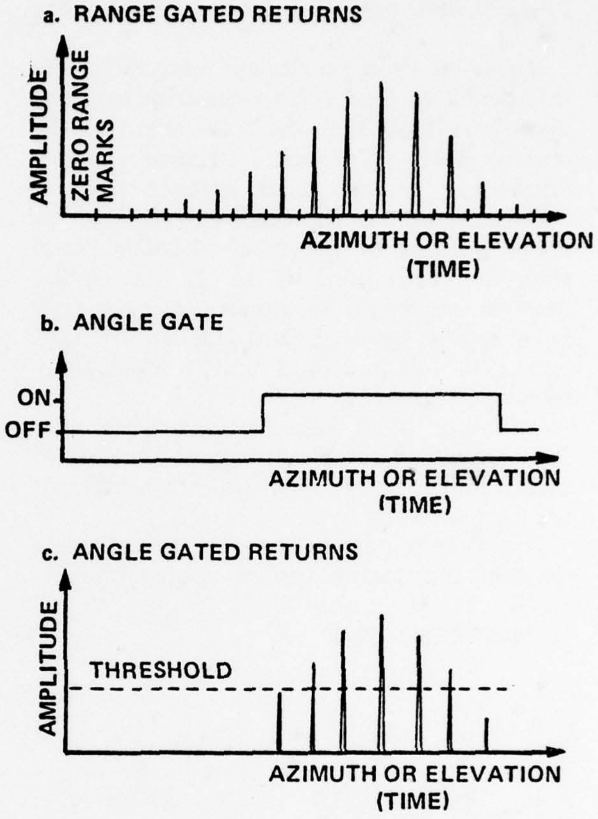


FIGURE 42. ANGLE GATING

The situation is slightly different for a mono-track radar. In this case the radar scan pattern is moved to place the target aircraft on its central axis. Now the range-gated return is always present, but its amplitude changes as the aircraft moves away from the axis. This amplitude change is detected as a modulation of the range-gated return and the tracking circuits reposition the scan axis to place the target on the axis. Since the aircraft echo is always present, angle gating is not used; rather, specific modulation detectors take its place.

Trackbreakers working against range or angle gate circuits are commonly called gate-stealers or repeaters. The basic program of all gate stealers is similar and consists of

[33] The precise techniques used are discussed in Merrill I. Skolnik, *Radar Handbook* (New York: McGraw-Hill Book Company, 1970), Chap 21, pp 38-45.

the following four steps. These steps are illustrated by Figure 43, which shows a range gate stealer.

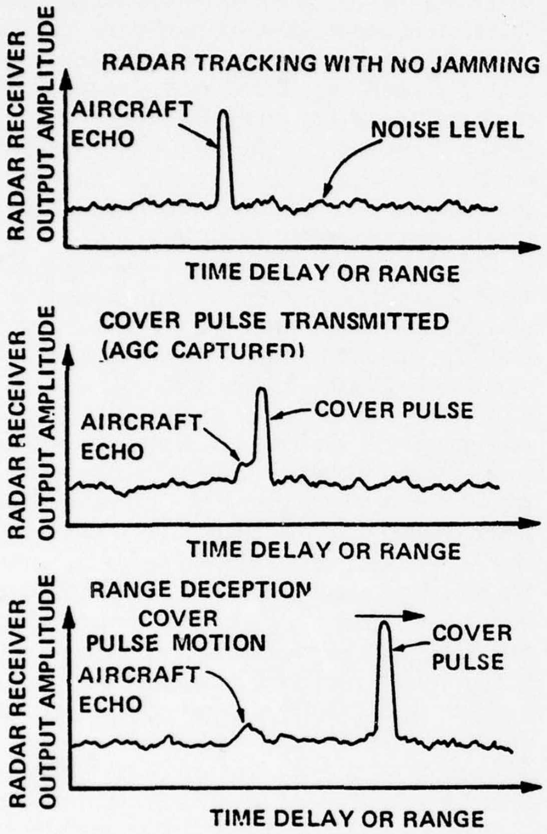


FIGURE 43. RANGE DECEPTION OF A TRACKING RADAR

a. The deceiver detects that the tracking radar has selected its aircraft as the object to be tracked.

b. The deceiver transmits a *cover pulse* whenever a radar pulse is received by its receiver. The cover pulse is a pulse designed to be much larger than the aircraft radar return. Since the radar tracking circuits are looking for the largest radar return in the vicinity of the aircraft, (i.e. within the range or angle gate) they will transfer to the cover pulse. Furthermore, the radar AGC circuits will tend to suppress the radar return since they will sense the cover pulse.

c. By a suitable combination of time delay and amplitude change, the position of the cover pulse is caused to move away from the aircraft position in azimuth, elevation, or range.

d. When the cover pulse is far enough away from the aircraft the track breaker is either turned off (return to step a) or the cover pulse repeats the program from step b. In the former case, the aircraft disappears from the tracking radar; in the latter, the radar attempts to follow a very erratically moving target. In either case the resulting tracking errors should result in large weapon miss distances.

If the radar is part of a mono-track system then track breaking in angle often uses inverse modulation. That is, when the radar signal increases the amplitude of the cover pulse is decreased and vice versa. Since the cover pulse is larger than the radar echo, the echo is suppressed by the AGC circuits and the tracking circuits sense only the cover-pulse moduation. But the cover-pulse moduation, being inverse to the real echo modulation, tends to drive the scan center line away from the target aircraft, thus introducing large tracking errors and hopefully preventing any tracking at all.

The simplest remedy that the defense system can use against track breakers is to have its tracking-radar operators switch to a manual mode of operation. This remedy is effective because a man watching a radar scope can discriminate between the cover pulse and the aircraft return; therefore, he can track the aircraft. But how does the operator know which is the aircraft return and which is the cover pulse? The answer lies in the fact that all deceivers incorporate some time delay—the time delay necessary for the received signal to be processed and actuate the transmitter. Thus the cover pulse initially must always be at a slightly greater range than the aircraft echo. Therefore a man watching the radar scope knows that initially the earliest pulse (even though small) is the aircraft.

Although manual tracking will largely counter a repeater jammer, manual tracking is never as smooth as automatic tracking. Thus the weapon miss distance will increase, increasing the probability of aircraft survival against non-nuclear defense weapons. For example, it is not uncommon for weapon probability of kill to drop 30 percent as a result of a switch from automatic to manual tracking.

Burnthrough. It should be noted that in all the discussion of deception, the basic relationships of the ECM problem have not changed. There will almost always be a range at which the radar echo will be equal to the deceiver signal. Thus, except for certain antenna patterns or for the case where the jammer is more powerful than the radar, there is always a minimum effective range for deception. We make a separate note of this fact because the common use of burnthrough range implies jamming, and it is easy to forget that deception is under the same constraint. This constraint is most important for track breakers since they will probably be employed at short ranges against a terminal threat and they rely on the cover pulse being significantly stronger than the aircraft echo. Thus with deception, as with jamming, the tactician must consider if this minimum range is going to hinder his mission plan.

Chaff

The primary reason for changing the electrical properties of the medium between the radar and the aircraft is to change the propagating characteristics of the atmosphere. To date very little attention has been given to substances which would change these basic propagation characteristics of the atmosphere, because it seems difficult to obtain a large effect without both requiring extensive dispersion of the material, and some very special properties.[34] What has been done is to use small metal strips of appropriate length which act as efficient reflectors of the radar energy.

Thus the second class of ECM consists almost exclusively of this approach. In the Second World War these strips were called *window*, but since that time they have come to be called *chaff*. Originally chaff consisted of thin strips of aluminum foil whose length was approximately a half-wavelength at the frequency of the radar to be countered. The strips were made thin to maximize the air resistance or drag and minimize the weight so that the chaff would fall very slowly. More recently, chaff has been made of glass or plastic fibers with a thin metal film deposited on their surface.[35] Since glass is less dense than metal, the resulting chaff falls more slowly than the older versions.

The dimensions and physical orientation of chaff is an important factor in its design and use. An analysis of the action of chaff shows that for maximum signal return one should make its length a multiple of one-half wavelength of the radar signal. This length maximizes the sympathetic electrical resonance effect, analogous to that which occurs with sympathetic vibration of a tuning fork or piano string. Unfortunately, the thinner the chaff the more pronounced and frequency specific the resonance effect. Furthermore the reradiated energy is strongest broadside to the individual chaff element, similarly to a tuning fork. In essence, each chaff element is a single dipole with a donut-shaped pattern similar to that of Figure 13.

Thus chaff is both frequency and orientation sensitive. Both of these characteristics are compensated for by the typically small cross section of chaff, for that means that large quantities of chaff can be packaged in a small volume. Thus, one can use chaff of several different lengths in the same package to be effective against radars of widely different frequencies. As for orientation, the small size of the chaff elements means that they are randomly oriented upon dispensing, thus their effectiveness becomes omnidirectional.

For use against low-frequency radars (50-100 MHz), the chaff must be very long (5 to 10 feet). In the second World War, it was found that lengths of up to 100 feet were effective over a wide frequency range and this

[34] Vakin and Shustov, *Osnovy Radioprotivodystviya*, pp 358-369, contains a discussion of this technique which is more useful in space.

[35] Dilpare, "Chaff Primer", p 46.

very long chaff, called rope, was extensively used. Because these long strips of aluminum have catastrophic effects on high voltage transmission lines, rope is prohibited from being dropped over the continental United States.[36]

Chaff is typically packaged in units about twice the size of a cigarette pack.[37] When this unit is dispersed in the atmosphere it creates a radar echo similar to that of a small aircraft. If a stronger echo is wanted, two or three units are dispensed simultaneously.

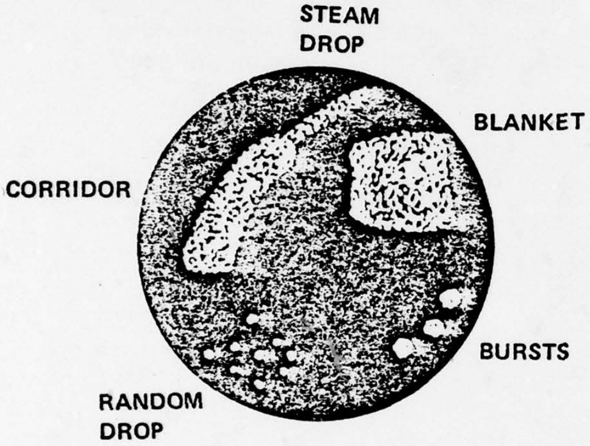


FIGURE 44. CHAFF EFFECTS

The effects produced by chaff depend upon the manner in which it is used (See Figure 44). If the bundles are dropped continuously (a *continuous* or *stream drop*) they will cause a long line of radar returns across a PPI scope. Several side by side stream drops will form a *chaff corridor* and an airplane flying within that corridor cannot be seen. If an area is covered with chaff it is sometimes called a *chaff blanket*. These uses of chaff constitute a form of jamming, but jamming that is localized in space and independent of the aircraft being protected. Thus the aircraft must fly through the space containing the chaff if it is to be screened.[38,39]

Chaff may also be used in a manner akin to deception. For example, if chaff bundles are dropped randomly (a *random drop*), the radar scope may become so filled with chaff returns that the radar operator has difficulty finding the airplanes. This technique is very similar to false-target generation. On the other hand, against a tracking radar chaff may be dropped in bursts of several bundles. These *chaff bursts* will create a larger radar echo than the dropping vehicle and the radar may tend to lock on to the chaff rather than the airplane. Thus we have a track-breaking technique.

With chaff, as with all deception techniques, there is the problem of target credibility. The breadth, width, and intensity of the chaff return can be adjusted by varying the number of bundles of chaff dropped at one time. But the problem of target motion is not so easily solved. Since chaff is deliberately made with a low mass to surface area ratio for minimum fall rate, it becomes stationary in the air mass immediately after dispensing. That is, the only reason that chaff returns move is by means of air mass movement, i.e., by wind drift.

In jamming usage the low speed wind drift is a nuisance but it is tolerable and it can be accounted for in planning. In deception through false target generation the slow movement means that a large number of chaff bundles must be dropped before there is any appreciable effect on the air defense system. Furthermore if the radar has MTI the chaff

[36] AFR 55-44, *Performing Electronic Countermeasures in the United States and Canada.*

[37] A typical chaff unit is approximately 1" x 3" x 5", weighs 7 to 16 ounces and contains many hundreds of individual pieces.

[38] Chaff suspended in air is essentially invisible. Thus staying within a chaff corridor or blanket can be difficult without using airborne radar.

[39] Because of the low density of chaff dispersed in the air, and the small mass of individual chaff dipoles, chaff ingested by jet engines has a negligible effect on the engine itself.

returns can be essentially eliminated. And in all these cases the dispensing aircraft is highlighted by the chaff trail behind it.

In the track breaking role, the chaff separates rapidly from the dispensing aircraft so large bursts must be dropped to insure that the radar will transfer to the chaff. Here the slow movement of the chaff may be an asset, because the chaff separates quickly from the aircraft. On the other hand, this rapid separation means that the chaff must disperse, or "bloom" rapidly so that the tracking radar will see both aircraft and chaff together and then transfer to the chaff. Aircraft maneuvers will help in this case since they change the tracking angular rates and tend to cause the radar to lock on to the chaff. If the radar is tracking the leading edge of the chaff stream in order to follow the dispensing aircraft, then the aircraft can fire chaff-dispensing rockets forward.[40] These will lead the tracking radar away from the aircraft for the life of the rocket. After the rocket runs out of chaff, the aircraft will return to the leading edge of the chaff trail as it flies out of the rocket chaff corridor, unless it fires another rocket.

In both these techniques the tracking radar may either break lock on the aircraft or its tracking performance may become very erratic, depending on the effectiveness of the technique. But if the tracking errors cause any weapon to miss the aircraft, the technique is successful. In any event, the low speed movement of chaff must be considered in planning its use.

Finally, there has been some suggestion in the literature that the radar signal will be weaker on the other side of the chaff cloud because of the energy reflected by the chaff.[41] Hence, a chaff corridor could be used as an attenuator to decrease the effective radar range. However, this idea needs to be thoroughly tested before much credence is placed in the effect.

Radar Cross-Section Modification

The third major class of ECM encompasses techniques to make the aircraft radar return either smaller or larger. One technique is to use proper design.

Because of resonance effects straight portions of aircraft skin greater than a half-wavelength in dimension will radiate

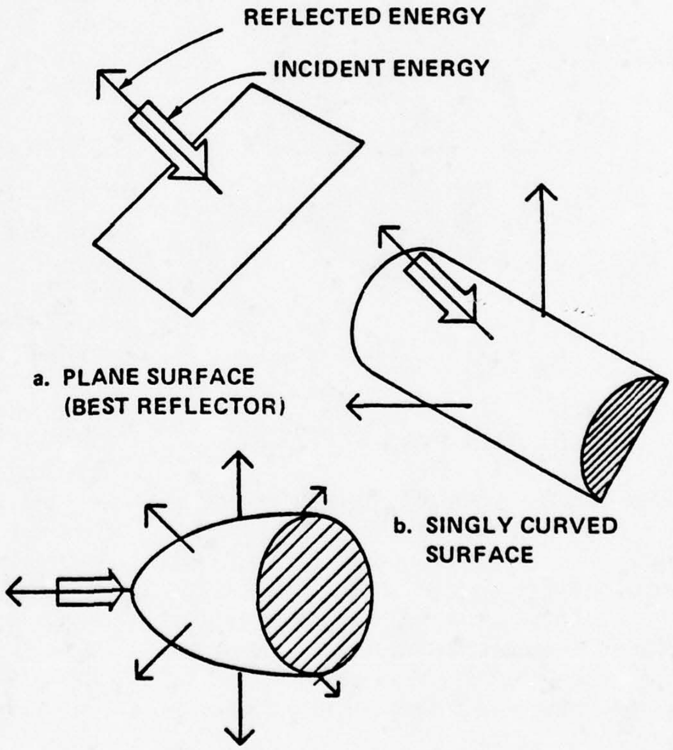


FIGURE 45. SURFACE REFLECTIVITY VERSUS CURVATURE

[40] Diplare, "Chaff Primer", pp 46-47.

[41] *Ibid.*, p 47.

perpendicular to the surface when illuminated by a radar (Figure 45). However, if the surface is curved the resonance effect is decreased and the resultant reradiation will be distributed in several directions. Thus cylindrical or ellipsoidal aircraft surfaces (curvature in one or two dimensions) give small echoes. Fortunately, doubly curved surfaces are aerodynamically desirable. On the other hand, the decoy, QUAIL, has flat sides in an obvious attempt to increase the radar return to the sides.[42]

This effect of surface curvature also means that the reflectivity of an airplane varies widely with the relative orientation of the aircraft with respect to the radar. If the aircraft is nose-on to the radar, then not only is the effective cross-sectional area minimum (to minimize aerodynamic drag) but the surfaces are most doubly curved and the major reradiation will be to the side. Thus the radar echo will be small for a monostatic radar. (One might suspect that a bistatic radar would be better in this situation.) However, when the aircraft is broadside to the radar it will look most like a flat surface, thus its radar echo will be largest for a monostatic radar. In practice it is not unusual for the broadside radar cross-section of an aircraft to be as much as 500 times greater than the nose-on cross section. And the effective cross section varies rapidly with change in aircraft attitude because of the complex interaction between the returns from the different structural parts of the aircraft (scintillation.) The typical nose-on radar cross-section of a small jet aircraft is 10 square meters or less while a large aircraft may have a frontal cross-section of 100 meters.

If we want to reduce the radar cross-section of an aircraft still further than that possible from design we must coat the aircraft skin with an electromagnetic absorbent material or radar absorbent material (RAM). One type of electromagnetic absorber is based on destructive interference between the reflected energy from different layers of the material.[43] The material must be a quarter wavelength thick and permeable by the electromagnetic wave; the reflection from the second (and possible succeeding layers) cancels the reflection from the outer surface. This effect is inherently narrowband so that making a RAM coating effective over a wide frequency range is difficult. The effect is the same as that used to make anti-reflection coatings on optical lenses.

A second type of RAM is one which dissipates internally the energy incident upon it.[44] This absorber is inherently broadband. Because both these techniques add both thickness and weight to the airframe they must be selectively used.

A third method of changing the reflective properties of an airframe is to use special reflectors. In particular, the *corner reflector* is a very efficient reflector. A corner reflector is formed from three intersecting, mutually perpendicular metal sheets. It reflects about as well as a single sheet of metal whose size is that of its opening, but it is effective over a wide range of angles, whereas the flat sheet is effective only perpendicular to its surface. With a corner reflector a small airframe can be made to look like a big bomber. Such a little airframe is called a *decoy* and is used to dilute an air defense system by causing the defense to think that the penetrating raid is larger than the number of strike aircraft.[45]

A fourth method of cross-section modification is to place a deceiver in the aircraft to return a signal that is bigger than the normal radar echo (an *echo enhancer*). This method is effective at long range where the echo will be weak, but there exists a burnthrough range for this technique, as for all active ECM

[42] R.T. Pretty and D.H.R. Archer, *Jane's Weapons Systems* (London: Jane's Yearbooks, 1970), p 162.

[43] Vakin and Shustov, *Osnovy Radioprotivodystviya,* p 370.

[44] *Ibid.*

[45] This is the reason for the proposal for SCAD—supersonic cruise armed decoy—with the additional feature that the decoy will contain a weapon. In effect the decoy becomes an air-to-surface missile (ASM) and the destructive capability means that the enemy cannot ignore the decoy even if he can distinguish it from the other aircraft.

techniques. Thus decoy discrimination is always possible close to radar, and the technique is successful in that region only if the defense does not have enough time to make use of that information.

Expendable Countermeasures

This term is often considered to be synonymous with chaff but in its broadest use covers several active and passive techniques. Its basic meaning is that of an ECM device which is used up in its employment. As such it includes not only chaff and decoys (with or without echo enhancers) but also expendable active ECM devices. These latter devices may be either jammers or deceivers, depending upon the particular effects desired.

The primary purpose of expendable active countermeasures is to achieve defense saturation by using a large number of jamming sources. Initially, it seems attractive to use such devices as an alternative to sidelobe ECM. A moment's reflection will show, however, that such use requires approximately the same total power as a single sidelobe ECM device[46], but this power is now delivered by many small units operating in concert. Hence, they face the dual disadvantage of potentially lower efficiency of RF power generation plus the necessity of delivering them in some area distribution which is close to optimum. So expendable ECM appears useful only if their employment can capitalize on the number of independent ECM sources presented to the defense.

Expendable active ECM sources do face three additional problems which must be overcome for widespread tactical employment. First, like chaff, they must be deployed by some means and the vulnerability of the deployment scheme can greatly affect the overall usefulness of the devices. Second, their period of activity must be managed. That is, being expendable they have a limited operating period and that operating period must coincide with the activity they support. Thirdly, if they are to be widely used they must both be cheap and have extended storage life.

ECM Tactical Concepts

Now that we have discussed the basic principles of ECM, how can we use ECM in an actual penetration of an air defense system? We shall discuss the two extremes, the single penetrator and the large raid.

Single Penetrator. The single penetrator is representative of a reconnaissance mission. Because there will be only one aircraft the penetrator is forced into a one-on-many situation which creates three problems for the penetrator: power, signal processing, and passive tracking. The ECM which surmounts these problems may have to be very sophisticated, but this mission is relatively infrequent and its importance is great, so the extra sophistication is worthwhile.

The power problem occurs because the radars will probably be on many different frequencies. If ECM is to be effective it must work against all the threats to the aircraft. Fortunately, one can establish a priority of threats:

1. Tracking Radars
2. Nearby Search Radars
3. Distant Search Radars.

The available ECM capability is allocated to the highest priority threats.

Tracking radars are accorded the highest priority since they are associated with some weapon system which presents an immediate threat to the aircraft. Such radars typically have only a short range capability so that the number to be countered at any one time is not too large. Even so the ECM equipment

[46] Receiving antenna gain in free space results from concentrating the energy sensitivity over a small area of the spherical surface. Thus the gain, G, becomes the ratio of the sensitive area to the total spherical area. To achieve a given power level at the receiver requires either P watts at the beam center or GP watts through the sidelobes. To give a constant ECM level over an antenna's total search area thus requires one sidelobe ECM device of GP watts or G P-watt ECM devices distributed over the spherical surface. This result will be modified somewhat by the particular radar sidelobe structure and the presence of the earth, but the conclusion is accurate in order of magnitude.

and tactics must be able to handle these in a multiple-threat situation.

Nearby search radars are second priority because they are likely to be passing acquisition data to tracking radars. Furthermore they are likely to be within burnthrough range so their data is relatively accurate. Again their numbers are few but they require the most jamming power, hence they should be countered if the capability is available.

Distant search radars are more or less spectators to the action. They add frequency diversity to the air defense system; but, if the penetrator carries enough power to jam every type of nearby search radar, then it has enough power to jam the distant ones also, so they can be generally ignored.

The signal processing problem is especially important to deceptive ECM because the single penetrator, by definition, has no accompanying aircraft to distract the defense. Because terminal threats will have the strongest signals due to their short range, it is tempting to process only the strongest signals and assume that this will solve the de-interleaving problem. But the defense may employ multiple terminal threats simultaneously to assure a kill, so automatic deceivers ought not become flustered or paralyzed by all this attention.

The passive tracking problem occurs if the penetrator carries sufficient noise jammers to conceal his aircraft from every radar. Tracking radars may then continue to guide their weapons to him by flying them out the strobes.[47] The detonation point of the weapon is unknown but if the weapon has a proximity fuse, it is likely to be effective. Search radars can also be used to determine the penetrators exact position by triangulation from two or three radars. Since there is only a single penetrator triangulation is not difficult.

One might consider using support jamming from other non-penetrating aircraft to aid the penetrator. However, these additional aircraft might alert the defense and take away any advantage of surprise that the single penetrator would have.

Large Raid. A large strike within enemy territory is representative of the many-on-many situation, wherein the air defense system must keep track of many aircraft. Although the number of threats per aircraft has not increased, the air defense system has to integrate data on many aircraft from many sensors to effectively control its weapons. Thus the data rate of the air defense system typically increases more than that of the penetrators. If this rate becomes great enough, the air defense system will begin to saturate. One of the results of saturation is that the time to react to each penetrator increases and this increase reduces the defense's ability to cope with the raid. Consequently, the problem areas shift to the defense so that with a large raid it is pertinent to discuss defense data rate, defense saturation and overall defense effectiveness.

The essence of the defense data rate problem is time, the time in which the defense must react. For example, the time required for a penetrator to reach its target is a rough measure of the time available to the

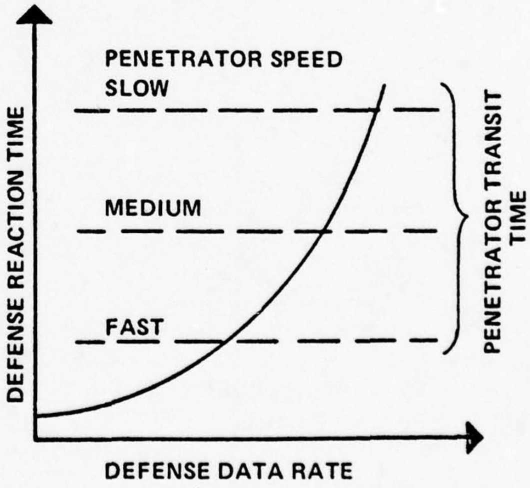


FIGURE 46. AIR DEFENSE MARGIN OF EFFECTIVENESS

[47] In SAM systems this is sometimes called *3-point guidance*—the tracking radar, the missile and the aircraft are kept lined up on a straight line.

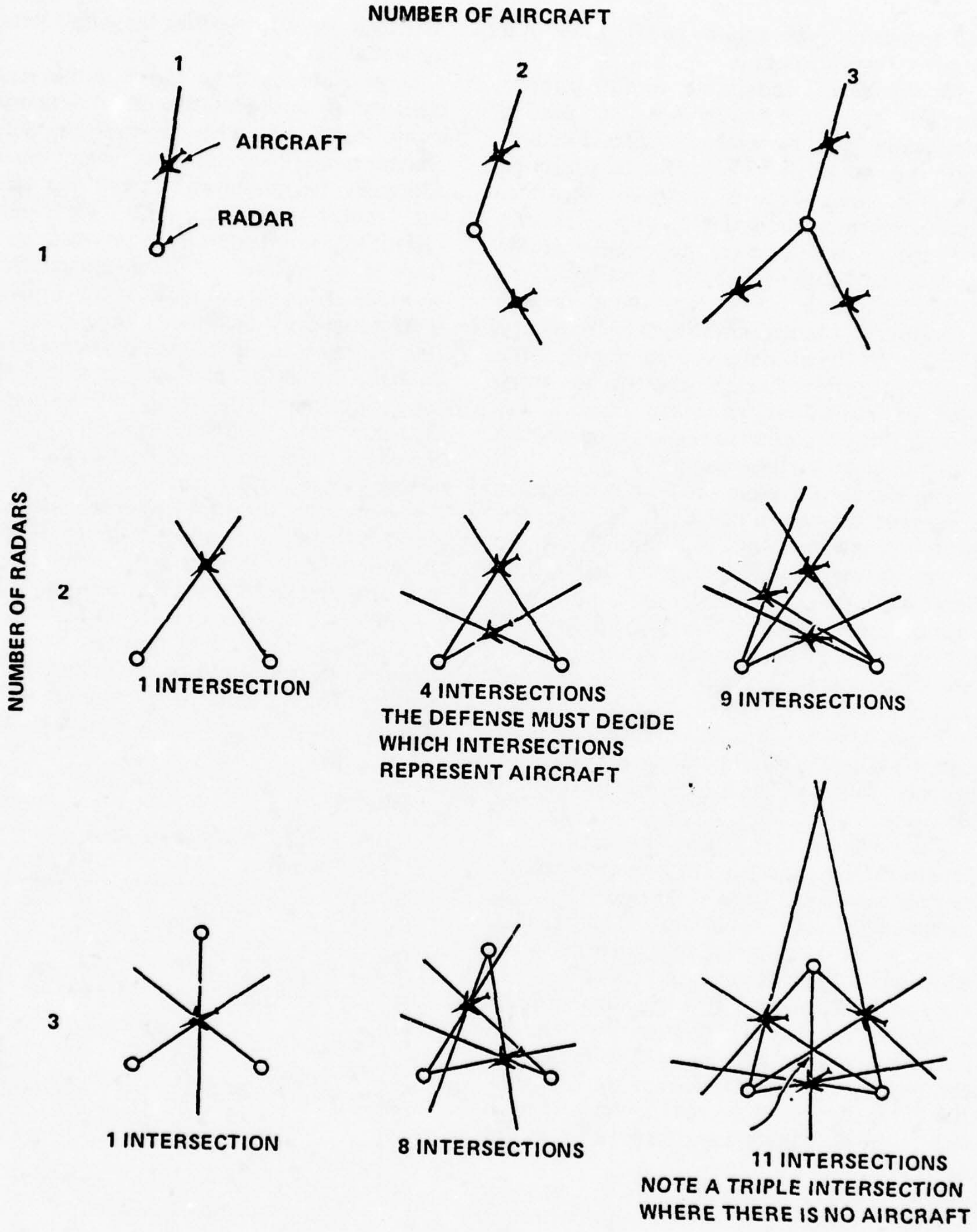


FIGURE 47. THE DEGHOSTING PROBLEM

the defense to react to that penetrator. As the defense data rate increases due to multiple penetrators the margin between the available reaction time and the data processing time decreases (Figure 46). Thus the combination of high speed penetrators and high data rate (many penetrators) could greatly reduce the effectiveness of the air defense system.

An impressive example of the data rate problem of the defense occurs when all the penetrators are able to effectively jam the search radars with noise jammers and the defense elects to passive track the penetrators. Figure 47 shows that for multiple passive sensors the number of possible locations of the penetrators is at least equal to the number of penetrators squared. Thus the defense has to decide which intersections represent aircraft. This problem, called the *deghosting problem*, has to be solved expeditiously if its solution is to be of use.[48] The magnitude of the problem is such as to be almost impossible of solution; thus, the defense will probably continue to seek active radar echoes.

The magnitude of the deghosting problem suggests that with a large raid the threat priorities may want to be changed initially by placing nearby search radars first and tracking radars second. It is obvious that when a penetrator is being tracked by a tracking radar his greatest immediate danger is from the tracking radar. But tracking radars have a restricted field of view, thus they have to be told where their target is. If they can be denied this acquisition information they are forced to search for their targets, a very inefficient process. Saturation of the air defense system will deny them their acquisition information and thus degrade their effectiveness.

How can an air defense system be saturated? The idea is basically this–provide the air defense system with more apparent targets than it can handle. In this case, the command and control function provided by the system is negated and each air defense weapon must fight by itself.

There are three ways of putting the air defense system into saturation. The first is to use large numbers of aircraft. The second is to destroy or otherwise physically render ineffective part of the system so that the remainder becomes saturated and ineffective. This concept is embodied in the idea of defense *roll-back*, the progressive destruction of the defense as the strike force approaches the target. The third way of saturating the defense is to use ECM to increase the apparent raid mass to beyond the saturation point. In this latter case one would use self-protection ECM, support ECM, chaff, and expendable ECM; the exact mix would depend upon what was available.

Lest we convey the wrong impression, there are alternatives to saturation. One might consider the feint to provoke the defense into premature reaction. This technique would be most useful against an area defense where launching the interceptors means that they are out of service after they land until they can be refueled and re-armed, "turned-around".[49] In other cases, it may be sufficient to ignore the area defense and plan ECM only against the terminal defenses. If the defense is very dense, one might want to consider a low-altitude penetration with the idea of denying the defense all radar information. Hence, the tactics used in a large raid can and should vary depending upon the tactical situation.

We can summarize this discussion of the large raid by drawing a diagram of the effects of our ECM on the air defense system as in Figure 48. The ordinate is the raid mass, which is the number of aircraft in a specified geographical area. The abcissa is the

[48] Note that deghosting is complicated by the fact that the strobes are sensed at different times due to radar scan patterns, thus there will probably be no accurate triple-strobe intersections, especially for high-speed penetrators. Furthermore, if the strobes occur randomly, either because of random reporting due to data rate saturation or ECM tactics, the situation could become very confusing.

[49] Price, *Instruments of Darkness*, contains numerous examples of feints. The largest was that used during the Normandy invasion, pp 201-209.

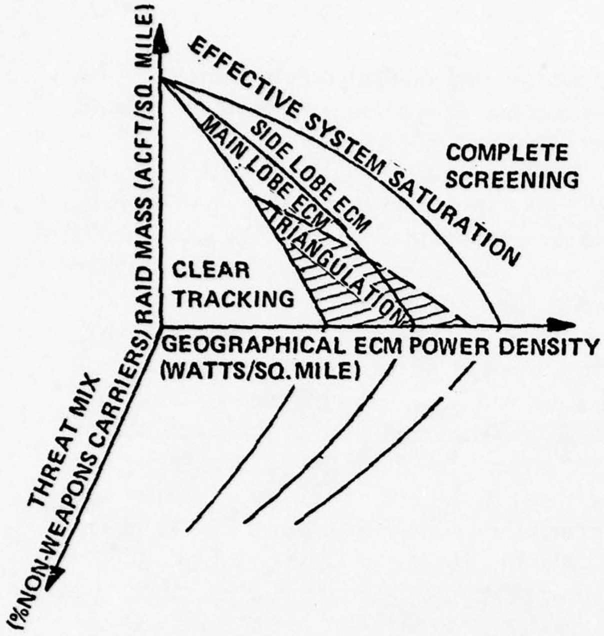

RAID MASS (ACFT/SQ. MILE)
EFFECTIVE SYSTEM SATURATION
SIDE LOBE ECM
MAIN LOBE ECM
TRIANGULATION
COMPLETE SCREENING
CLEAR TRACKING
GEOGRAPHICAL ECM POWER DENSITY (WATTS/SQ.MILE)
THREAT MIX (%NON-WEAPONS CARRIERS)

FIGURE 48. THE EFFECTS OF ECM ON AN AIR DEFENSE SYSTEM

geographical ECM power density.[50] This density is a measure of the effective jammer power, since it is related to the individual jammer powers summed at the radar antennas. The third dimension is some measure of the threat mix, i.e. the combinations of strike aircraft, decoys, support ECM aircraft and air-to-surface missiles. This last axis not only measures the diversity of the ECM effects generated but it also measures the defense motivation to track and kill the intruders.

The effects of the ECM on the defense portrayed in the abcissa-ordinate plane shows the major effects of ECM on the defense. The boundaries, of course, are not sharply defined and they undoubtedly depend upon the particular techniques used. Nevertheless, having made this generalization about ECM and air defense systems, it would be useful to be able to flesh it out by putting numerical values on the figure. When we try to do this, however, we come face to face with one of the basic problems of ECM analysis–how do you measure threat mix, raid mass and ECM geographical power density.

Figure 48 gives one approach to threat mix measurement, measuring the percentage of weapons carrying vehicles or its complement. This is obviously not the only measure that could be used, but we will not pursue it further because the measure used depends upon the sensitivity of the defense to various perceived threat mixes.

Of more interest because of their direct relationship to ECM effects are raid mass and geographical power density. Because we are considering ECM effects at a very high level of aggregation we need to change our point of view. Our previous discussion of ECM has been almost entirely in terms of geometry in a limited geographical area, with some discussions of relative numerical strength. But when we talk about a large raid we have such a wide range of geometries that we want to aggregate to some sort of mass or density measure. Hence we come to the problem of what is the relevant geographical area to use?

The area to use seems to be the intersection of the defense coverage area and the ground area within line-of-sight of all the raid aircraft (Figure 49). These two areas are to be computed at the altitude of the highest aircraft in the raid including its supporting aircraft, for example, including any support ECM. We compute the raid mass and the geographical power density by counting the total number of aircraft and the total jammer power in this area respectively. These figures give some indication of the magnitude and complexity of the problem facing the defense, hence they should relate to overall defense effectiveness.

Support ECM. In any tactical situation support ECM is usually used when the strike aircraft do not have enough available power, space or payload to carry sufficient ECM to protect themselves. The support aircraft may

[50] This is different from the power densities commonly encountered, *viz.* spectral power density (watts per megahertz) and radiated power density (watts per square meter).

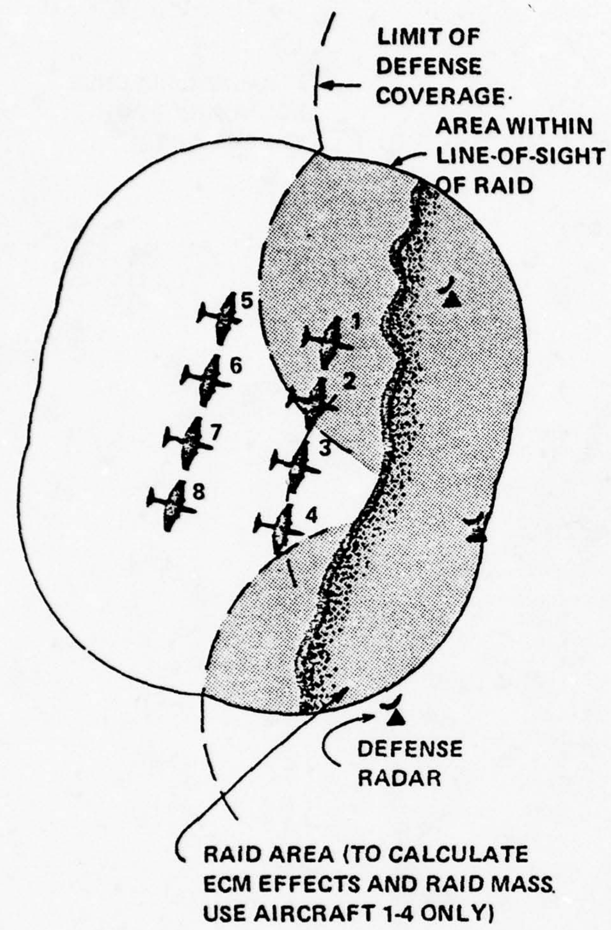

LIMIT OF DEFENSE COVERAGE
AREA WITHIN LINE-OF-SIGHT OF RAID
5
6
7
8
1
2
3
4
DEFENSE RADAR
RAID AREA (TO CALCULATE ECM EFFECTS AND RAID MASS. USE AIRCRAFT 1-4 ONLY)

FIGURE 49. THE AREA USED FOR RAID MASS CALCULATIONS

or may not accompany the strike aircraft, the decision being a compromise between the greater effectiveness and greater vulnerability of the escort aircraft.[51] In any event the use of support aircraft raises three additional considerations which the strike planner must address.

First, support ECM in general requires more power than self-protection ECM since it must rely on jamming or deception through the radar sidelobes. In this respect stand-off ECM needs the most power since it must work into the radar sidelobes to protect penetrators which are much closer to the radar than it is.

Second, if the support ECM is effective then the support aircraft must be well protected. For each support aircraft protects several strike aircraft; if it were to be shot down then the rest of the striking force would be exposed. Hence, effective support aircraft are valuable targets to the defense and their safety cannot be assumed.

Third, support ECM should only be considered when it is essential to the mission and when its addition does not greatly increase the mission cost. This principle is slightly different from the more appealing practice of insisting that no more than 50 percent of the aircraft contribute only support. Historically, support ECM has been most used on large raids as exemplified by our World War II experience.[52] However, Appendix C shows that gravity dropped conventional weapons, with their large CEPs incur a large attrition cost to destroy a target. Thus using a large number of well-protected (low attrition) support aircraft does not affect the mission cost contributed by the strike aircraft losses. But if one could insure accurate weapon delivery, it would pay to use 75 percent or more of support aircraft to insure the strike aircraft could survive to achieve certain target destruction.

A Typical Penetration

As an example of the employment of the ECM principles discussed above, let us consider a strike mission against the fighter airfield of A. (This airfield is adjacent to the LARGE BANG radar against which the ELINT mission of the last chapter was run. See Figure 50). Two squadrons of 20 fighter-bombers each will be employed, supported by six stand-off jammer aircraft

[51] The most critical part of the mission in this regard may be the egress from the target area. At this point the strike aircraft have dropped their ordinance and are "clean" and thus capable of high speed. But the support aircraft are still carrying their electronics payload of ECM so they may not be able to stay with the strike aircraft, thus leaving both groups of aircraft with degraded protection.

[52] Price, *Instruments of Darkness*, pp 179-198.

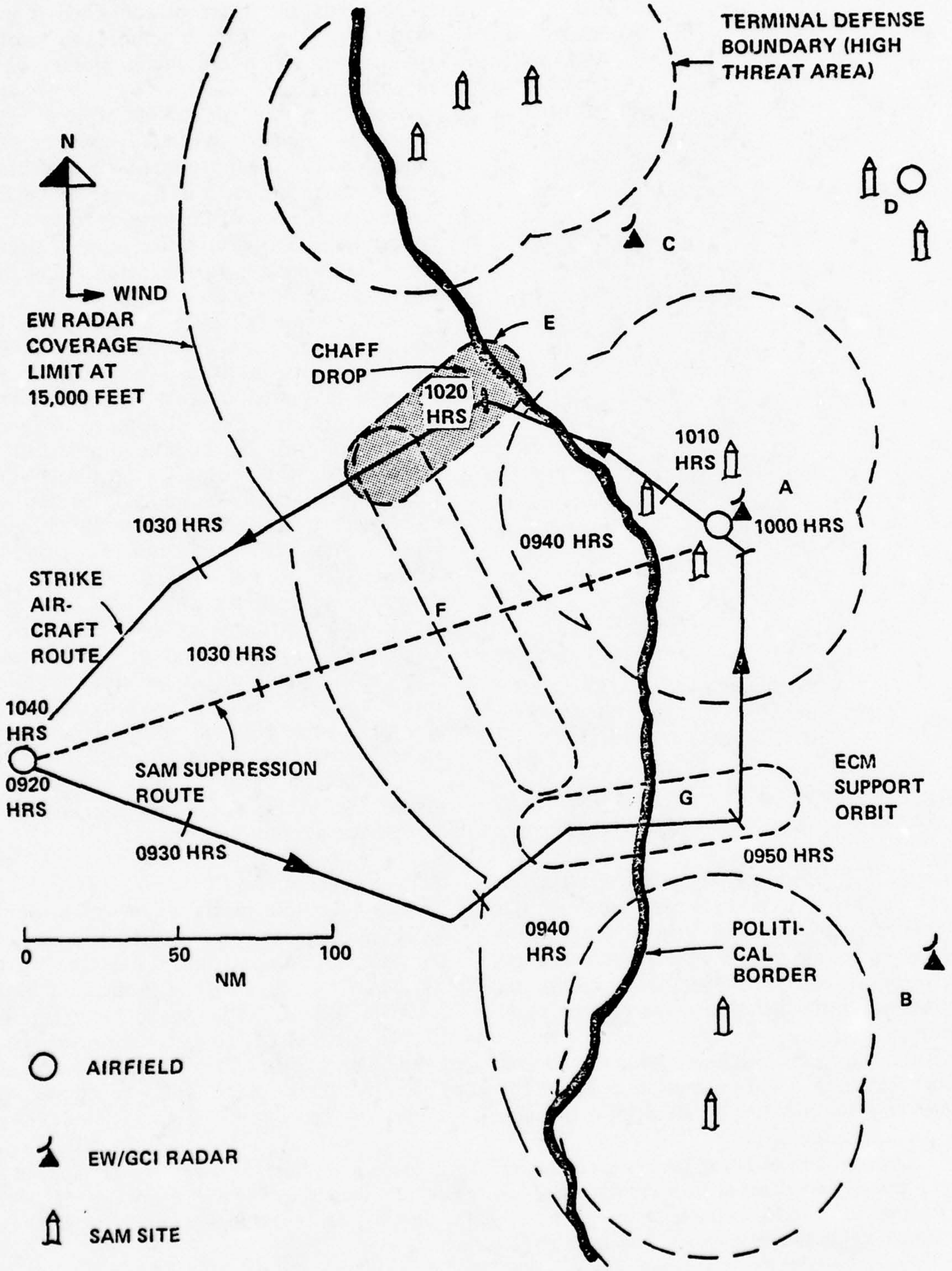


FIGURE 50. A TYPICAL PENETRATION

flying in two orbits. In addition, three more ECM aircraft will make a chaff drop to cover the egress of the strike aircraft from the target area. The strike aircraft will carry self-protection jamming against the terminal defenses in the target area, *viz*, AAA and SAM. In addition, they will carry ECM for use against interceptor AI radar and radar air-to-air missiles and IR flares for use against IR missiles. (IR countermeasures will be discussed in Chapter 8).

We will assume that all the fighter bombers are single seat except for the four SAM suppression aircraft. The latter carry an EWO and extra ECM equipment for the purpose of precisely locating active SAM sites and either destroying them or forcing them into ineffective modes of operation. Because of the restricted space and crew on the fighters, all their ECM must be preset before takeoff. Thus data from extensive aerial reconnaissance must be available.

The ECM support aircraft, the standoff jammers and the chaff laying aircraft will be transport aircraft which have been specially configured for this role. The will also carry extra crew members to operate the ECM equipment. Since these aircraft are relatively slow and have no defensive weapons they shall be accompanied by a fighter combat air patrol (CAP) to protect them against enemy interceptors. This is necessary since they are essential to the protection of the strike aircraft. In addition, these aircraft will be routed so as to avoid all SAM defenses.

The ECM support aircraft also need good ELINT data, especially on the LARGE BANG radar at A since it will be primary GCI control for the interceptors. ELINT data on the radars at B and C (Figure 50) is also necessary so that they can be effectively jammed. Because the EOB of the battle area is known the ECM support aircraft need carry only jammers against the threats listed. This will allow them to carry more than one jammer against each radar and thus increase their effectiveness. In addition, the ELINT will allow the chaff to be selected for greatest effectiveness against the radars.

The stand-off jamming patterns have been selected to jam radars A, B and C over as much of the strike route as possible. In addition, the patterns have been designed to avoid the high threat areas since the transport aircraft are defenseless against SAMs (except for ECM). Finally their patterns have been selected to penetrate the border as little as possible to minimize the danger from interceptors.

We shall assume that the fighter-bombers maintain an average speed of 560 knots and the ECM support aircraft an average speed of 420 knots. The fighter-bomber squadrons will be called the first and second squadrons.

Let us consider a typical mission sequence. The attack is scheduled for 1000 hours to allow the attack to come out of the sun. (Such considerations are easy to fulfill in hypothetical examples.) We shall start our sequence at midnight.

0000 hours Aircraft arming and loading begins. Three ECM support aircraft are loaded with chaff, 40 percent of which is cut to cover the frequencies of the LARGE BANG radar (2.4–3.2 GHz). The ECM support aircraft jammer load is about 40 percent spot jammers effective against LARGE BANG. However, jammers effective against the SAM acquisition and missile control radars are also included. The ECM load of the fighters contains only ECM against the SAM missile control radars, AAA radars, and AI radars. The fighters also carry flares against IR missiles.

0730 hours Premission briefings begin. Intelligence reports that the EOB is as shown in Figure 48, with three SAM sites protecting the airfield and the radar site. Interceptors at D can be expected to respond to the attack. These interceptors will probably be voice controlled. The observed radar frequencies of the radars at A, B, and C are briefed as well as the SAM frequencies. Since a SAM suppression flight will be in the target area, strike pilots are briefed that SAM sites may launch their missiles before turning on their missile control radar. (This reduces the time the radar is on the air and thus lessens the possibility that the site will be attacked by an anti-radiation missile (ARM).[53] The mission includes the use of a feint. ECM support aircraft will drop chaff and jam in pattern E to force the defense to react to an anticipated threat from the northwest although the strike will come in from the south. The chaff corridor will also provide some protection for the returning strike aircraft. The stand off jamming patterns have been laid down to jam the radars at B and C also.

0900 hours ECM support aircraft take off. Four head to the northeast toward pattern E and climb to 20,000 feet. The other five head to the southeast toward pattern G at 10,000 feet.

0910 hours The flight of four SAM suppression aircraft from the second squadron take off and head directly toward A at 5,000 feet.

0920 hours The strike aircraft from the first squadron take off and climb to 15,000 feet along the strike route.

0930 hours Sixteen strike aircraft from the secon squadron take off and climb to 15,000 feet along strike route. The ECM support aircraft begin dropping chaff and jamming in pattern E. The intent is to create a diversion and to provide a chaff corridor to protect the strike aircraft upon return from the target. Pattern E requires 20 minutes to complete. The other ECM support aircraft begin climb to 13,000 feet–(three aircraft), and 17,000 feet–(two aircraft) in a small orbit at the eastern end of pattern G. At 5 minute intervals beginning at 0930 hours they start pattern G.

0940 hours The aircraft from the first squadron enter enemy radar coverage. All ECM support aircraft in pattern G begin jamming all EW/GCI and SAM acquisition radars on the air. The SAM suppression flight crosses the border and climbs looking for SAM missile-control radars.

0950 hours First squadron aircraft turn inbound to target. Second squadron aircraft enter enemy radar coverage. One ECM support aircraft enters pattern F from pattern E and climbs to 40,000 feet to jam upper beams of LARGE BANG. Other aircraft in pattern E continue sowing chaff. All ECM aircraft jam any missile-control radars detected.

1000 hours First squadron at IP, second squadron turns inbound to target. ECM support aircraft in pattern G begin to enter pattern F.

1010 hours First squadron comes off the target and heads for pattern E. Any crippled aircraft proceed directly to the border.

1020 hours Second squadron comes off the target. First squadron enters chaff cloud and turns for home.

1030 hours Second squadron turns for home in chaff cloud. SAM suppression flight descends and heads home. SAM suppression flight has been instructed to deliver their remaining gravity weapons against LARGE BANG site if possible. First squadron leaves enemy radar coverage.

1040 hours Second squadron leaves enemy radar coverage. SAM suppression flight is out of radar coverage. All ECM support aircraft turn for "home plate". ECM support aircraft continue to jam all enemy radar signals detected.

1110 hours All aircraft are on the ground.

1130 hours Mission debriefing begins. Crew members relate the significant defense

[53] An ARM missile is an air-to-ground missile designed to passively home on the signal from a radar site. It is an example of the use of the ECM principle of destruction. In this case the small lethal radius of its necessarily small warhead is compensated by the low CEP of its electronic guidance system.

> behavior, especially that different from anticipated in the premission briefings. For example, the SAM suppression flight indicates that a fourth SAM site was active. EWO's on ECM support aircraft received indications that interceptors from the airfield at D were controlled by a data link rather than voice. Pilot reports indicate that the LARGE BANG site was damaged, the runway at A was cratered and five fighters were destroyed on the ground. A photo reconnaissance flight will overfly A later in the day to verify these reports.

ECM in Air Defense

Up to this point we have considered ECM solely from the vantage point of the attacker; the defender has had only the option of responding to ECM, that is, ECCM. However, with the advent of more sophisticated airborne electronic systems this traditional division of roles can change. If the attacker uses radiating electronic systems for navigation, bombing or command and control then the defender may initiate ECM against these systems. So let us discuss each of these applications of ECM in turn.

Navigation. We are here defining navigation as the process of getting close enough to the target to allow employment of weapons delivery systems. ECM against these navigations systems is usually called *meaconing*,[54] a term which was coined in the Second World War.

The vulnerability of radiating electronic navigation systems arises not from any inherent design limitations but from their operational usage. For unless the system is designed specifically for weapons delivery applications, it is likely to be designed without any ECM resistant features because a navigation system to be otherwise economically justifiable must be employed over a wide area by many different types of users. That is, a navigation system will be used in the rear areas by many administrative aircraft as well as by strike aircraft in the forward area. With so much of its use completely under friendly control, the inclusion of ECM resistant features is not especially likely when acquisition cost is minimized, as is often the case. Thus ECM resistant electronic navigation systems are likely to be a rarity.

Another factor stemming from wide use which contributes to ECM vulnerability is that the system will be exposed to the enemy, especially in times of peace.[55] Thus the enemy will have a relatively leisurely opportunity to study it and devise effective ECM.

The payoff of ECM employment against electronic "Navaids" varies depending upon the reliance placed upon the navigation system by the attacker. It can vary from complete negation of the attack, as exemplified by the British use of meaconing in World War II, to mild harrassment. The general effect is to increase attrition by making avoidance of the defense more difficult, because precise navigation becomes more difficult.

Terrain Following/Terrain Avoidance. Two special attack navigation systems are the terrain following and terrain avoidance systems.[56] These are usually aircraft radar systems used to enable a low flying aircraft to overfly or detour around hills and mountains on the way to the target. Since an attack aircraft flies low over mountainous terrain only to avoid the air defense system and/or surprise the enemy, ECM against these systems tends to deny this advantage. Furthermore, these automatic systems are only required if night or bad weather attacks are contemplated, since clear-weather, low-level flying is one of the skills expected of a tactical fighter-bomber pilot. So ECM

[54] See Chapter I

[55] A prime example is the TacticalAir Navigation (TACAN) system, which has been incorporated into the Air Route Traffic Control (civil air navigation) system.

[56] Terrain following insures that the aircraft maintains a minimum clearance over all obstructions in its predetermined route of flight. Terrain avoidance allows the aircraft to maintain minimum altitude by flying around hills and mountains, or over them at minimum altitude if the pilot should so elect.

directed against such a system will be employed when the attacking pilot is psychologically least able to withstand it.

Of the two systems, terrain following is generally the most vulnerable since it has only one response—fly up. Thus any signal injected into the receiver will tend to make the aircraft more visible, and more vulnerable, to the defense. Terrain avoidance, on the other hand, has two options: it can either fly up or detour around the apparent obstruction.

Although ECM against these systems has potentially high payoff in increased attrition, it is not easily employed. For the low aircraft altitude means that the reception range of terrain avoidance/terrain following systems is limited. And since their route into the target area is unfettered by terrain, widescale ECM against these systems can be costly.

But near the target cheap ECM has a potentially high payoff. For this high cost system is only cost-effective if it is used against targets whose priority is high enough to make attacking them with an expensive system worthwhile. Thus the defense need only employ the ECM around high value targets, with the objective of making the attrition rate high enough to discourage this type of attack. Such a use is enhanced by the fact that blind bombing systems are usually less accurate than visual bombing, thus more sorties will be required to achieve a given level of damage to the target.

Weapon Delivery. The third area of ECM employment by a defense is against radar bombing systems. The objective of this use is to confuse the attacker so that he cannot drop his bombs accurately. Unfortunately, this use has to contend with the natural effect of terrain. That is, the well-trained bombadier will use all the terrain features surrounding the target to guide him. In fact, he need not see the target at all, since offset bombing capability allows him to use some feature near the target for bombing guidance. Consequently, the prime prerequisite for this employment of ECM is high power, so that the terrain is completely obscured to the aircraft bombing radar, and its major use would be to protect extremely high priority targets.

Command and Control. The final area where ECM can aid an air defense system is against electronic command and control systems. These systems are more communications systems than sensor systems, hence they are more easily protected with some ECM features. However, they are used in an operational environment where rapidity of communication is important and the message to be sent has little direct meaning relative to future operations. Thus sophisticated ECM features are not worth the effort, especially since they may be compromised if an aircraft is shot down. All this makes for relatively vulnerable systems, especially since the defender has a power advantage. Nevertheless, if the attack is well planned, command and control communications are minimized. The upshot of all this is that ECM against the attacker's airborne command and control may be widely variable in effectiveness. It is most effective if there must be a large amount of airborne coordination for the attack, and a large part of its effectiveness may be psychological, adding to the already severe stress of combat.

ECM Design Philosophy

In view of the wide diversity of ECM effects and the wide range of systems against which ECM can be employed, is there any way that ECM can be designed to avoid both quick obsolescence and a complete reliance upon an ability to respond quickly to enemy threats? There are potentially three avenues of approach. The approach chosen depends upon both the threat and the available technology.

The first is to use ECM signals of the simplest type and widest applicability. Ideally these signals should be effective against the majority of systems employed by the enemy. Since noise is the inescapable natural interference in all electronic systems, then it appears that this approach dictates a reliance on noise (jamming) as the primary ECM to be used throughout the fleet. Deception would tend to be limited to special high priority missions conducted over a short time span.

The second approach would be to emphasize the use of low cost ECM for fleetwide use. Then the total cost of protection could be kept low. This approach would emphasize mechanical ECM such as chaff, and again would deemphasize specialized, sophisticated deceivers, since they are typically high cost.

The third approach is more equipment oriented. It recognizes that as much as we dislike it, reaction to the enemy is an inescapable fact of electronic warfare. Thus we should try to make reaction as easy and inexpensive as possible. There are two methods to accomplish this. The first is to modularize the equipment so that substitutions can be made easily. This method does not necessarily reduce the cost of each module, nor does it help if capability–modules–must be added to an aircraft which has a full suit of modules. And the total cost is reduced only if we buy less than a full suit of modules for each aircraft so equipped. Such a procedure anticipates that not all aircraft will need a full suit simultaneously, so that we can time-share some modules between two or more aircraft.

The second method uses a new design approach, architecture if you will, for ECM. In this approach one builds receivers that are generally capable of detecting a wide variety of signals, and high power transmitters which are capable of radiating a wide variety of ECM signal modulations. These receivers and transmitters ideally would cover the total ECM frequency spectrum, or lacking that, they could be modularized to cover the spectral regions containing the important threat systems. But their important feature is that basically they would not be threat specific. Instead, the modification and specialization of these systems against specific threats would be done by insertable elements, either printed circuit boards to do the specialized signal processing, or punched cards if digital computer control is possible. The objective of this approach would be to make the specialization of the equipment cheap and easy. Of course, increasing total capability will always be difficult, but this approach has the potential to make the modification of existing capability relatively easy.

In addition to these three approaches there is one additional approach which has a great effect on ECM, even though it is not ECM related; namely, all efforts that improve the weapon delivery accuracy of the attacking aircraft. A large factor in force attrition has to be the necessity to go back and restrike repeatedly targets that are not destroyed on the first strike. This aspect of air warfare has been recently highlighted by the advent of "smart bombs" in the Southeast Asia Campaign.[57] It seems clear that if the probability of successful target destruction is high, not only does our ECM have less exposure to the enemy–so that he has less opportunity to develop counter-countermeasures–but we can also afford to better protect the forces that we use, because the drain on our reserves due to continual employment is reduced. Thus ECM benefits doubly from all increases in strike effectiveness.

In conclusion, well-considered ECM design philosophy offers some real payoffs in allowing us to cope with the future electronic threats. However, to realize these payoffs we must do some concentrated thinking as to what are the best approaches in each situation.

[57] See Appendix C for a discussion of air defense attrition.

Chapter 6

ELECTRONIC COUNTER-COUNTERMEASURES

Electronic counter-countermeasures is the art of reducing the effectiveness of an EW threat with the objective of making the cost of effective EW prohibitive for the enemy. As in ECM, ECCM includes both radar design and operator training. The radar ECCM designer must understand the various forms of ECM that his radar is likely to encounter, hence he is very interested in intelligence about the ECM threat. Likewise the radar operator would like to know what ECM he will encounter. But in both cases detailed intelligence will probably be lacking. Therefore, the designer must provide a variety of options to be used against the expected threats. And the operator must be trained both to recognize the various countermeasures which might be used against him and to select the appropriate combination of options against each of them. The most effective measure to combat ECM is an up-to-date piece of equipment operated by a well-trained operator.

Radar Design

Radar design for ECCM can be broken down into three areas: Basic radar parameters, signal processing techniques, and design philosophy.

Basic Radar Parameters. Basic radar parameters are those radar parameters which influence the transmitted radar pulse: power, frequency, PRF, pulse length, antenna gain, antenna polarization and antenna scan. These parameters are fixed by the radar design and cannot be changed without major change of the radar. Hence, the ECCM capabilities of a radar are often decided early in the design phase.

For a ground radar, *power* is often considered the fundamental ECCM parameter. The British have even made this into a proverb "It is more blessed to transmit than to receive".[1] In this view ECM becomes a power battle with the outcome going to the stronger, more powerful opponent. Airborne jamming equipment is limited in size and weight and therefore has a power limitation. Hence, in this view the advantage always lies with the ground radar. Unfortunately, this view ignores the fact that the power battle occurs not between the output stages of the radar and of the ECM transmitter, but between the ECM output and the radar echo reflected from the aircraft. Hence, there are a number of other ECM and ECCM options available to sway that battle.

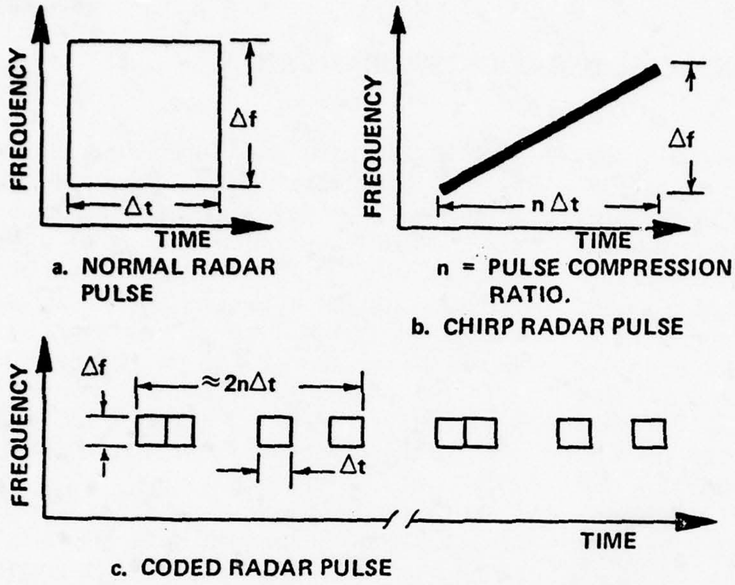
For example, two of the options available to the designer of pulse radars which have direct implications for the power battle are pulse coding and pulse compression. In a pulse radar, the maximum pulse power or peak power is ultimately limited by voltage breakdown in the transmitter. However, any good radar textbook will show[2] that pulse energy is the prime determinant of target radar detectability. Thus any technique which increases radar pulse energy by lengthening the length of the pulse is an ECCM technique. Specifically, the techniques of pulse coding and pulse compression, as shown in Figure 51, effectively increase radar pulse energy but by different amounts. Both techniques use the ideas of correlation detection or matched filtering to maintain the range resolution while allowing pulse energy to increase.[3]

Pulse coding substitutes a burst containing n pulses in a unique pattern lasting approximately 2n pulse widths for a single pulse. Pulse compression expands the basic pulse with a non-linear filter to a continuous pulse n times as long. Both techniques increase the

[1] Stephen L. Johnston, "Military Radar–Weapon System Analysis", (Course lecture notes on Principles of Radar, Georgia Institute of Technology, 18 Sep 1970), p 4.

[2] See, for example, Skolnik, *Introduction to Radar Systems*, pp 56-430.

[3] Skolnik, *Radar Handbook* devotes Chapter 20 to pulse compression radar.



a. NORMAL RADAR PULSE

n = PULSE COMPRESSION RATIO.

b. CHIRP RADAR PULSE

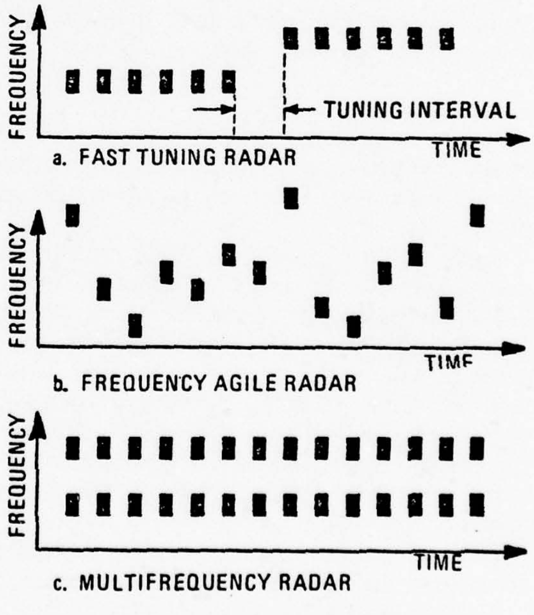
c. CODED RADAR PULSE

FIGURE 51. CODED RADAR PULSE CHARACTERISTICS

duty cycle of the radar at the expense of a shorter resting time. Thus both techniques will increase the minimum range of a monostatic radar, but the increase will be greater for a pulse coded radar. On the other hand pulse coding has potentially the simpler signal processing scheme since it can be implemented with linear digital technology. It is suspected that pulse coding has not been widely used because of the constraints imposed by high power modulator design.

For airborne radars versus ground ECM, the ECM in theory can always win the power battle if it has unlimited primary power. But an airborne ground-mapping radar looks at an extensive fixed target (the earth), in contrast to a ground search or tracking radar which looks at a mobile point target. Thus the airborne radar can use terrain and man-made features at a distance from the target, so power is not the sole determinant. (Further, a single, fixed ground jammer makes an excellent navigation aid.) In the case of airborne radars versus aircraft, both operate under the same constraint and the outcome is not obvious.

Frequency becomes an ECCM design parameter through the ability of a radar set to transmit on more than one frequency. Using state-of-the-art components and techniques the designer may make the frequency shift of the radar very fast and automatic. By constantly monitoring the received frequency spectrum (by some sort of spectrum analyzer) the radar operator will know what channels are being jammed and what channels are clear. The operator then may select [4], within the operating frequency range of the radar, a channel clear of jamming. This technique is most effective if the radar operator can monitor his transmitted spectrum also so he can match the radar spectral maximum to the ECM spectral minima. (Note that here both the radar



a. FAST TUNING RADAR

b. FREQUENCY AGILE RADAR

c. MULTIFREQUENCY RADAR

FIGURE 52. RADAR FREQUENCY CHARACTERISTICS

[4] This means that the radar transmitter must be broadband and the operating frequency selected within this band. A narrow band transmitter must *tune* to a new frequency, a lengthy, time-consuming process.

operator and the ECM operator are monitoring the frequency spectrum). Radars having these features may be called fast tuning radars, frequency agile radars, or multifrequency radars. Figure 52 illustrates the distinction between these terms.

Another way of using frequency as an ECCM technique is to cause the frequency of the radar pulse to vary during the duration of the pulse (Figure 51). This technique frequently results in extending the pulse length so that one effectively achieves greater transmitted pulse energy due to the long pulse without increasing the peak power of the transmitter. Such radars, often called CHIRP radars or pulse compression radars, make ECM difficult because of the greater energy per pulse; the frequency variation within the pulse also gives the receiver a means of distinguishing the target echo from ECM.[5]

A third method is seen in the doppler radar, including radars designed for MTI signal processing. The actual ECCM advantage is gained from signal processing inserted in the receiver, but the intention to use the doppler frequency shift must be reflected in the transmitter design. For example in a pulse-doppler radar the transmitter must often be designed to radiate a very stable frequency. Table 18 compares the different techniques as to their implied ability to change frequency.

Table 18

Frequency Changing Capability of ECCM Techniques

Technique	Time to Change Frequency[1]	Remarks
Coded Pulse	Long (seconds or minutes)	No returning capability implied
MTI/Doppler	Long (seconds or minutes)	Frequency shift sensed in receiver only
Multifrequency/Diplex	Long (seconds or minutes)	Multiple frequencies transmitted simultaneously, no special ability to change them implied
Fast tuning[2]	Medium (seconds)	Retuning process shortened but still requires many pulse intervals
Frequency Agile[2]	Short (milliseconds)	Each pulse on different frequency
CHIRP[2]	Very short (microseconds)[3]	Frequency change within pulse

[1] Time to change transmitter frequency implied by the technique itself. If techniques are combined (e.g. agility and MTI) the capability of the faster technique applies. But the upgrading of the slower technique is likely to require a major increase in cost and complexity.

[2] Note that tuning, agility and CHIRP imply order of magnitude differences in the time to change frequency and consequently, significant changes in sophistication and complexity.

[3] Although CHIRP radars change frequency very rapidly within each pulse, they may not be able to change the swept frequency band between pulses.

Usually *PRF* is not considered as having much influence on ECCM

[5] CHIRP, or pulse compression, is basically a correlation technique similar to that of the matched filter. It maximizes the received pulse voltage amplitude after processing while leaving noise (and also ECM that doesn't contain the precise frequency variation used) essentially unchanged.

capability. In general, high PRF radars are more resistant to jamming because the average radiated power is greater.[6] Changing the PRF on a random basis would seem to be a good counter to deception, but because PRF is related to the basic timing of the radar system, this technique is impractical. Some radars do switch periodically between two different PRFs; but this technique, called staggered PRF,[7] is primarily used as a means of improving MTI performance by eliminating some blind speeds.[8]

We have already noted that *pulse length* may be changed to raise the radar average power, and hence the ability to detect aircraft. However, lengthening the pulse reduces the radar range resolution, the ability to separate targets at the same azimuth and close together in range. Hence, pulse lengthening is only used where range resolution is not important, such as an early warning radar, or where the pulse can be coded or compressed.

Good *antenna design*, as reflected in low sidelobe levels, is an ECCM design technique, because it prevents a jammer or deceiver from affecting the radar at many azimuths. Low sidelobe levels also make the job of anti-radiation missiles more difficult since there is less chance of the missile homing on the radar unless the radar is pointing at the missile.

Antenna *polarization* can be used to discriminate between ECM and aircraft because the aircraft ECM antennas may not have the same polarization as the radar wave reflected off the aircraft.[9] To take the greatest advantage of this effect the radar should have the capability to change its polarization to obtain the best discrimination. Such a capability is especially necessary because aircraft are complex shapes so that the polarization required for best discrimination will change with the aspect of the aircraft as seen by the radar. As an example, circular polarization is often used by air traffic control radars to discriminate against precipitation echoes (rain showers).[10]

Finally, the radar *scan pattern* can influence ECCM capability because it influences the amount of energy directed toward the radar target. For example, a height-finding radar is usually more ECM resistant than a search radar because its sector scan illuminates an aircraft more frequently than a search radar's circular scan. A phased array radar might be quite ECM resistant because its ability to rapidly scan its radar beam in an irregular manner would give the ECM little warning. And there are other techniques in which the transmitted beam does not scan, scanning is done only by the receiver and its antenna. In this case the ECM has no direct access to the radar scan pattern and thus has difficulty using that information to interfere with the radar system operation. Into this class fall the *passive detection* and *home-on-jam* techniques where the "radar" does not transmit but uses the ECM energy emitted by its victim to determine the victim's location, often by triangulation from two or more separate locations.

Signal Processing Techniques. Signal processing techniques are usually functions which are incorporated into the radar receiver. Although certain signal processing techniques may place constraints on the transmitter many of them can be added to the receiver after the radar has been built. These techniques are often called ECCM or *anti-jamming* (AJ) fixes since they were initially developed as retrofits to improve existing

[6] If target detection were performed on a pulse by pulse basis this statement would be false. But invariably the effect of several consecutive target returns are summed (or integrated) in either a special circuit or by the display scope phosphor itself before the target detection criterion (threshold) is applied. This processing enhances the signal more than the noise, and the higher the PRF the greater the enhancement during the time the antenna is pointing at the aircraft. Thus high PRF radars are harder to jam as a general rule.

[7] Note that staggered PRF can be considered a pulse coding technique to improve radar velocity performance.

[8] Skolnik, *Introduction to Radar Sytems*, pp 129-131.

[9] Since aircraft antennas must meet aerodynamic criteria, their polarization may well be restricted.

[10] Skolnik, *Introduction to Radar System*, pp 547-551.

equipment. Some of our more recent radars, however, have tended toward a more sophisticated design concept in which the AJ devices are included in the basic radar system.

Signal processing techniques fall into a variety of categories. We shall only consider a few of them which are commonly used. Table 19 lists over a hundred ECCM techniques and is included to show the tremendous variety available.

Most ECM is very similar to some form of radio frequency interference

Table 19

ECCM Technique List

- Acceleration Limitation
- Angle Sector Blanking
- Angular Resolution
- Audio Limiter
- Aural Detection
- Autocorrelation Signal Processing
- Automatic Cancellation of Extended Targets (ACET)
- Automatic Threshold Variation (ATV)
- Automatic Tuner (SNIFFER)
- Automatic Video Noise Leveling (AVNL)

- Back-Bias Receiver
- Baseline-Break (on A-Scope)
- Bistatic Radar
- Broad-Band Receiver

- Coded Waveform Modulation
- Coherent Long-Pulse Discrimination
- Compressive IF Amplifier
- Constant False Alarm Rate (CFAR)
  - Cross-Gated CFAR
  - Dispersion Fix (CFAR)
  - IF Dicke-Fix CFAR (Dicke-Fix)
  - MTI CFAR
  - Unipolar Video CFAR
  - Video Dicke-Fix CFAR (Dicke-Fix)
  - Zero Crossings CFAR
- Contiguous Filter-Limiter
- Cross Correlation Signal Processing
- CW Jamming Canceller

- Detector Back Bias (DBB) (Same as Detector Balanced Bias)
- Dicke-Fix
  - Clark Dicke-Fix (Cascaded Dicke-Fix)
  - Coherent MTI Dicke-Fix
  - Craft Receiver
  - Dicke Log Fix
  - IF Canceller MTI Dicke-Fix
  - IF Dicke-Fix CFAR (Zero Crossings Dicke-Fix CFAR)
  - Instantaneous Frequency Dicke-Fix
  - Noncoherent MTI Dicke-Fix
  - Video Dicke-Fix CFAR
- Diplexing
- Doppler-Range Rate Comparison
- Double Threshold Detection

- Electronic Implementation of Baseline-Break Technique

- Fast Manual Frequency Shift
- Fast Time Constant (FTC)
- Fine Frequency
- Frequency Agility
- Frequency Diversity
- Frequency Preselection (Narrow Band-Width)
- Frequency Shift

- Gain Control
  - Automatic Gain Control (AGC)
  - Dual Gated AGC
  - Fast AGC [FAGC][1]
  - Gated FAGC
  - Instantaneous AGC
  - Manual Gain Control
  - Pulse Gain Control
  - Sensitivity-Time Control [STC][1]

- Guard-Band Blanker

NOTE: Data obtained from Stephen L. Johnston, "Military Radar–Weapon System Analysis" (Course lecture notes on *Principles of Radar*, Georgia Institute of Technology, 18 September 1970.)

[1] Added by the editor.

- High PRF Tracking
- High Resolution Radar

- IF Diversity
- IF Limiter
- Image Suppressor
- Instantaneous Frequency Correlator (IFC – CRAFT)
- Integration
  - AM Video Delay Line Integration
  - Coherent IF Integration
  - Coherent (IF) Integration (Moving Target)
  - Coherent (IF) Integration (Stationary Target)
  - Display Integration
  - FM Delay Line Integration
  - Noncoherent (video) Integration
  - Pulse Integration
  - Video Delay-Line Integration
- Inter-Pulse Coding (PPM)

- Jamming Cancellation Receiver
- Jittered PRF

- Kirbar Fix

- Least Voltage Coincidence Detector
- Linear Intra-Pulse FM (CHIRP)
- Lin-Log IF
- Lin-Log Receiver
- Lobe-on-Receiver Only (LORO, also SORO)
- Log Fix (Also, Log FTC)
- Logarithmic Receiver
- Logical ECCM Processing

- Main Lobe Cancellation (MLC)
  - Monopulse MLC
  - Polarization MLC
- Manually Aided Tracking
- Manual Rate-Aided Tracking
- Matched Filtering
- Monopinch
- Monopulse Tracker
- MTI
  - Area MTI (Velocity Filter)
  - Cascaded Feedback Canceller (MTI)
  - Clutter Gating (MTI)
  - Coherent MTI
  - Noncoherent MTI
  - Pulse Doppler
  - Pseudocoherent MTI
  - Single-Delay Line (MTI Canceller)
  - Re-Entrant Data Processor
  - Three-Pulse Canceller
  - Two-Pulse Canceller (Single-Delay Line MTI Cancellation)
- Multifrequency Radar
- Multisimul Antenna

- Phased Array Radar
- Polarization Diversity
- Polarization Selector
- Post Canceller Log FTC
- PRF Discrimination
- Pulse Burst Mode
- Pulse Coding and Correlation
- Pulse Compression, Stretching (CHIRP)
- Pulse Edge Tracking
- Pulse Interference Elimination (PIE)
- Pulse Shape Discrimination
- Pulse-to-Pulse Frequency Shift (RAINBOW)
- Pulse Width Discrimination (PWD)
- Pulse Length Discrimination (PLD)

- Random-Pulse Blanker
- Random-Pulse Discrimination (RPD)
- Range/Angle Rate Memory
- Range Gating
- Range Rate Memory

- Scan-Rate Amplitude Modulation
- Short Pulse Radar
- Side-Lobe Blanker
- Side-Lobe Canceller
- Side-Lobe Reduction
- Side-Lobe Suppression (SLS)
- Side-Lobe Suppression by Absorbing Material
- Staggered PRF

- Transmitter Power
- Two Pulse Autocorrelation

- Variable Bandwidth Receiver
- Variable PRF
- Variable Scan Rate
- Velocity Tracker
- Video Correlator

- Wide-Bandwidth Radar

- Zero-Crossings Counter

1E

(RFI).[11] Therefore techniques effective in reducing RFI are likely to be effective ECCM techniques also. As a general rule, good radar design practice reduces the vulnerability of any radar receiver to ECM and RFI. More practically, good design procedure implies that *proper shielding* and *power line filtering* are included in the receiver. Skimping in the design to reduce cost often increases the radar vulnerability to ECM.

Good radar receiver design is based on maximizing the ratio of received signal energy to noise power per hertz. Normally the bandwidth of the radar receiver is optimized to match the spectrum of the transmitted pulse.[12] Optimizing radar receiver bandwidth will also make jamming more difficult by reducing the effective power (power in the radar bandwidth) of a barrage jammer or requiring more accurate frequency set-on of a spot jammer. One could make the radar even more ECM resistant by minimizing radar bandwidth through using a long radar pulse, in which case one would gain an additional benefit from the increased energy per pulse. This is especially desirable if the radar is peak power limited, however, the decreased range resolution makes this approach unattractive except for early-warning radars, unless some compensating pulse compression technique is used in the receiver.

An important measure for reducing the effects of either ECM or mutual interference is to avoid saturating or overloading the receiver with large interfering signals. That is, the receiver should have a *wide dynamic range*. Linear rather than square-law detectors are therefore preferred. Another technique to achieve wide dynamic range is the *logarithmic receiver*, where the receiver gain is reduced for strong signals to prevent saturating the detector.

Doppler radars, including radars with MTI signal processors, although not designed specifically for ECCM purposes, are quite ECM resistant. Since doppler radars (pulse and CW) operate on the frequency shift caused by a moving target, they automatically filter out returns from non-moving targets, and consequently eliminate many unwanted signals, such as those from chaff. Some will even discriminate between returns from objects of different velocities such as an aircraft in a chaff cloud. This technique can also make deception more difficult, since the deceiver must imitate the proper frequency shift.

The MTI processor is a specific type of the general class of processors known as *correlation detectors* or *matched filter* receivers. These devices use the known characteristics of the transmitted radar pulse, such as the frequency variation of the CHIRP radar or the frequency shift caused by radial target motion, to discriminate against ECM and other interference.

In radar with *automatic threshold detection*[13] (in which the target is said to be present when the receiver output crosses a preset threshold) the presence of a jamming signal can increase the rate of false alarms (false targets) to an intolerable extent. If the radar output data is processed in an automatic device such as a computer, the device might be overloaded by the added false alarms due to jamming. Thus, it is important that the receiver present a constant false-alarm rate. Receivers designed to accomplish this are called *CFAR* (constant-false-alarm-rate) receivers.

If an operator were employed to monitor the radar output, the effect of the additional false alarms could be reduced by having the operator turn down the gain of the receiver during the presence of jamming, or else he might be able to ignore those sectors containing ECM. In an automatic threshold detector the same effect may be obtained by

[11] RFI is used to designate unintentional interference. For example, many electric shavers will severely interfere with AM radios.

[12] Reducing receiver bandwidth below the optimum bandwidth reduces both radar range and radar range resolution.

[13] The section on CFAR, as well as some other material in this chapter is based on a tech training manual published by the Technical Training Center, Keesler AFB, La.

using the average noise level to provide an automatic gain control, much as an operator would be adjusting a manual gain control. Because the automatic CFAR circuit reacts faster, it is superior to an operator in keeping the false-alarm rate constant, especially when the radar is subject to noise jamming from only a few azimuth sectors.

A CFAR receiver, no matter whether it is an automatic device or an operator controlling the receiver gain, maintains the false-alarm rate constant by reducing the probability of detection. When the threshold level is raised to maintain a constant false-alarm rate, marginal echo signals which might normally be detected do not cross the higher threshold and are lost. Therefore, *CFAR does not give immunity to jamming; it merely makes operation in the presence of jamming more convenient by making the receiver less sensitive*. If the jamming were severe enough, the CFAR, for all intents and purposes, could produce the same effect as turning off the receiver.

Design Philosophy. Design philosophy determines which ECCM techniques are incorporated into a radar and how they are interfaced with the rest of the system. This topic is broken out separately because it encompasses such other problems as the comparative cost of the techniques, the integration of radars using these techniques into the total defensive or offensive system, and the optimization of radar performance in the presence of ECM.

For example we can consider the problem of radar design to combat the effects of jamming using the concepts of the mathematical theory of games. It has been shown, under certain assumptions, that the optimum strategy for both the radar and the jammer is to spread their power evenly over the entire radar band and for the radar to employ a matched-filter receiver.[14] This is based on the assumption that both the radar and the jammer consider the radar post-detection signal-to-noise ratio as the measure of radar performance. The radar designer wishes to maximize the signal-to-noise ratio, and the jammer designer wishes to minimize it. Any deviation from the optimum strategy by either the jammer or the radar can only make a change for the worse. If other measures of radar performance are considered, the optimum strategies can be different.

The above optimization does not tell one how much power to use, just how to employ the available power. However, the strong influence of power on ECCM capability results in a corollary to the British proverb mentioned earlier, namely, increasing receiver sensitivity is not an ECCM design goal. For the maximum receiver sensitivity results in a minimum detectable signal equal to the thermal noise level. But ECM invariably adds extra noise to the receiver forcing it toward its upper limit of saturation. Thus the price of increased receiver sensitivity is wasted as far as ECCM is concerned. According to this corollary CFAR, which reduces receiver sensitivity, is not an undesirable ECCM technique.

A general rule of thumb for ECCM radar design is to incorporate unpredictable operating parameters, a "bag of tricks." The more orderly a radar is in its operation, the easier it is to predict what the radar is going to do or how it is going to operate, consequently the job of applying an ECM technique effectively becomes simpler. ECM becomes more difficult, however, if the characteristics of the victim radar are constantly changing. The parameter which may most easily be varied to confuse the ECM operator is the frequency. The capability for operator variation of pulse length, PRF, modulation and antenna characteristics is not commonly built into the radar, but different radars of the same type might be built with different values of these parameters to make ECM more difficult. However, one

[14] The careful reader will note that this policy appears to be the opposite of that advocated under signal processing techniques, i.e., narrowing receiver bandwidth to reduce jamming power. However, the signal processing comment was really to avoid *excess receiver* bandwidth. The policy advocated here implies some pulse compression or decoding scheme such that the noise-like radar signal is reconstituted as a pulse while all other (jamming) signals are transformed into noise-like signals.

would have to consider the advantage of this type of ECCM against the disadvantage of having to operate and maintain many nonstandardized radars.

The most common way of introducing unpredictability into radar design is through frequency diversity. Early radars were all designed to operate in a few specific frequency bands, where narrow-band jamming would render them all ineffective. New radar systems are designed so that each different radar type operates in a different frequency band[15] (Figure 53). The use of a much greater portion of the spectrum, from VHF to SHF (A to J Band), forces ECM operators to cover this total spectrum if they are to be effective. The effect of having to cover the total radar spectrum is usually to be able to put less ECM power against a single radar because the airborne platform is limited in its total power capability.

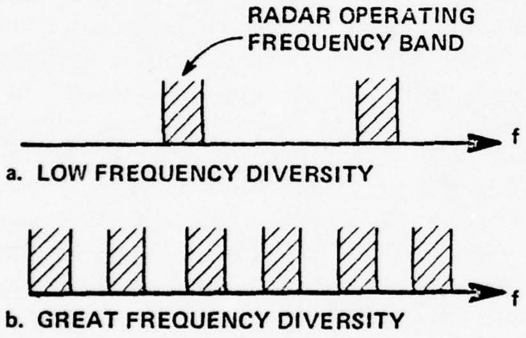

RADAR OPERATING FREQUENCY BAND
f
a. LOW FREQUENCY DIVERSITY
f
b. GREAT FREQUENCY DIVERSITY

FIGURE 53. FREQUENCY DIVERSITY

Another way of introducing randomness into ground radar systems is to make the systems mobile. Then the airborne platforms are never certain where the radars are located even after extensive reconnaissance, so that they cannot plan attack tactics based on fixed locations. Mobility has the effect of returning the element of surprise to the defense, but the defense pays the price of a power limitation because the mobility requirement limits the size of the units (generators, transmitters, antennas, etc.) which can be built. Mobility also makes integration of the radar into the air defense system more difficult since the radar location after movement is uncertain until the site coordinates are accurately determined. Thus it is difficult to decide when the mobile and the fixed radars are viewing the same aircraft if the mobile site location is not accurately known.

An important aspect of ECCM design philosophy is the relationship between automatic equipment and the human operator. The trained radar operator fulfills a useful and necessary role in a countermeasure environment and cannot be completely replaced by automatic detection and data processors. An automatic processor can be designed to operate only against those interfering or jamming signals known *a priori*; that is, any capability against such signals must be programmed into the equipment beforehand. New jamming situations not designed into the data processor might not be readily handled. On the other hand, a human being has the ability to adapt to new and varied situations and is more likely to be able to cope with and properly interpret a strange new form of interference than can a machine. Therefore, a skilled operator is the most important counter-countermeasure for maintaining radar operation in the presence of deliberate and clever countermeasures.

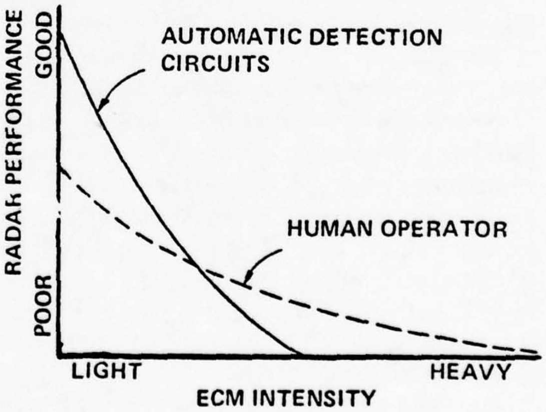


FIGURE 54. RADAR PERFORMANCE IN THE PRESENCE OF ECM

[15] The restriction of radars to operate in specific frequency bands is dictated both by the practice of using standardized electronic components and the limited frequency range of many of these components.

The previous comment can be generalized to say that one should not design a radar without providing the potential for manual operation by an operator in the event the automatic signal processing and detection circuits fail. The basic concept is that of Figure 54 which is a simplification of Figure 23. Although automatic circuits may do better than a man in a clean (non-ECM) environment, a man will continue to perform in ECM intensities where automatic devices fail. Hence, a good ECCM technique is to provide alternate modes of operation which can be selected by an operator. In general, all possible levels of degraded operation discussed in Appendix C should be provided.

Radar Netting

Up to this point we have been discussing counter-countermeasures which are applied to a single, isolated radar. But a single isolated radar almost never exists, there are at least two or three feeding information to a central point where the air-battle manager directs the conflict in the air. This combination of radars, often called a radar net, increases the potential ECCM capability of the system, but it also adds some constraints on the radars.

The first advantage of an air defense radar net is that it allows for frequency diversity. This practice of operating radars in many different frequency bands[16] immensely complicates the ECM problem since the attacker must counter every frequency if he is to succeed in denying the defense accurate tracking information. Of course, this advantage is not free, since the defender must pay the technology cost to develop radars in different frequency bands.

A second advantage of radar netting is that it allows the defender to do triangulation based on passive detection. Now passive detection as a technique does not require a radar set, a receiver that is trainable in azimuth is sufficient, but it does require a net of at least two and preferably three or more stations. If one is going to establish a radar net then this net can also function as a passive detection net for a small increase in cost.[17] Of course, a separate net has more redundancy, but the comments on the deghosting problem in Chapter 5 should indicate that a purely passive detection net has severe problems if the number of emitters is large. Thus it makes sense to combine both active (radar) and passive data in one place so that each can help the other.

The practice of radar netting has one serious problem and that is data rate control. Unless the centralized control has infinite capacity (which has a infinite cost) there is an upper limit to the amount of radar data that it can process and still "keep up" with the air battle. Thus netted radars must have some sort of data rate control as an ECCM device or the system can be saturated. If the radar data extraction is done manually (by radar operators) then data rate control is implicit since a man is limited in his information processing rate. However, if the radar data extraction is done automatically then data rate control is a necessity, since automatic circuits are not discriminating unless so designed.

Furthermore, with automatic processing one has to consider the problem of data management: Does the system tend to throw away good data and keep bad? This problem is complicated by the fact that in a heavy ECM situation the defense is looking for the marginal radar returns, those that are just barely seen, in order

[16] Note that frequency diversity differs from frequency agility and fast tuning in that the radars are spaced much further apart than their tuning range.

[17] For example, if the system uses automatic target detection the strobe detection equipment must be added to the radar.

to minimize the number of invisible attackers.[18] Thus we would like an automatic system to work as far down into the noise, as close to its noise threshold,[19] as possible. Such a requirement may require quite sophisticated and costly electronics since one would like not to raise the threshold if possible (as CFAR and most other ECCM fixes do).

An appreciation for the data rate control problem may be gained by considering an example. Consider a search radar with a one degree beamwidth and assume we wish to determine range to within 1000 feet or 1/5 of a mile. (I.e. we assume that we have a 2 microsecond pulse width.) If the radar has a 200 mile maximum range, then we are requiring that a target be determined to be within one of 360,000 range-angle cells of dimensions 1 degree by 1/5 mile. From information theory we know that locating a target in one cell requires 18.5 bits of information. If the radar scans at 6 rpm then the data rate from the radar is 111 bits per second per target, assuming that the target location function is done once every scan. Theoretically, the radar can produce information at a maximum rate of 40 megabits per second if there were a target in every range cell.

A more realistic tactical situation might have 100 aircraft within the radar's maximum range. In this case information is being produced at a rate of 11,100 bits per second. If we wish to send this information throughout the net over telephone lines then we are theoretically limited to a data rate of about 6,000 bits per second per line, and practically we may be limited to rates of one-half that.[20] Thus we have already encountered a data rate limitation and we have not even transmitted the data to a central processing point, or *filter center*.

Now if the filter center receives inputs from 10 radars over telephone lines, then it is receiving 30,000 bits of input information per second. This input rate is of the order of magnitude of that of a magnetic tape input to a digital computer, so it is not unreasonable. But if the tracking and intercept calculations are done by a computer, then there is a considerable amount of processing that must be done to this data. It is not hard to see that the computer must either throw away input data in an attempt to stay up-to-date, or lag further and further behind the air battle. Fortunately, less data is needed to maintain an established aircraft track than to initiate a new one, because the possible future locations of the aircraft are predictable from past data. However, the decrease in input data requirements may be partially compensated by the increased memory and computation required to use the recent track history.

If we add ECM to this example we increase all the data rates. If data control was necessary before, it is absolutely essential now. But in the process of throwing away data, what does the defender discard? Unless the controls are very "smart" the defense could easily discard good data and retain bad data. This is especially true if the defense wishes to work as far down into the ECM and noise as possible, because that philosophy will

[18] This a statement of optimal defense policy under the assumption that there are adequate numbers of weapons and there is no escort jamming but that every attacker has only self-protection jamming. Clearly if there is effective escort jamming the jammers are high priority targets because their loss will expose the remainder of the attacking force. The importance of this point depends upon whether the defense is a strategic or tactical defense. In strategic defense, the goal is maximum total losses for a single raid, so that jamming aircraft become preferential targets because of the data rate problems they cause. But in tactical air defense, attrition is a worthwhile and easier to attain goal, since attacking the exposed aircraft ("stragglers") may impose high enough loss rates on the penetrators to seriously curtail their effectiveness.

[19] The radar noise threshold is commonly understood to be the point at which the noise energy and target energy at the time the target echo is received are equal, often called the "tangential sensitivity." If the target echo is weaker than this threshold it is not detected.

[20] These rates can be increased by sophisticated modulation processes but the price is a higher quality (more noise-free) and more costly circuit.

result in large amounts of bad data in the system leading to very high data rates.

One way of solving the data rate control problem is to switch to passive tracking. Now the "bad data" from the point of radar detection becomes good passive tracking data. However, if the netted air defense system switches completely to passive tracking or triangulation, then it must solve the deghosting problem discussed in Chapter 5 and this may be as bad as trying to operate with bad data. A more promising approach seems to be to mix both passive and active data in the system, using the active data to eliminate ghosts and then maintaining track continuity with passive data.

Another solution to the data rate control problem is to use radar operators to filter the raw radar data before it is passed to the filter center. A man is a very severe data filter and he will preforce keep the system data rates low, on the order of 10 bits per second.[21] Of course we must be concerned about saturating the man we are using as a filter. However, his judgment as enhanced by training makes the human an adaptive data filter. Thus he is able to change his characteristics in response to the tactical situation in a way that no automatic system can. Consequently, human operators not only keep the data rate low, but they can select the best data for processing and in this way avoid saturation.

For this reason it appears that a completely automatic air defense net is undesirable, since the unique judgment of the human operator is needed for data rate control. Hence, in a military air defense system much of the system effectiveness depends upon the operator and his training.

Operator Training and Tactics

Given a well designed radar set with a large number of ECCM options, the outcome of the ECM-ECCM battle may well depend on operator training, if an operator is available. The corollary of this is that radar may not be useful in situations where an operator is not available. As an example, one might question the usefulness of a complex air-to-air interception radar in a single-seat aircraft on the basis that pilot would not have time to achieve optimum radar performance even if he knew how.

Given that a radar operator is present then it is obvious that he must have thorough training in the use of his equipment. This will include not only a thorough understanding of how to operate the radar itself, but also of ways of operating the set–tactics. One effect of training is to increase the J/S ratio at which radar detection or tracking can occur. We might diagram the effect of training as in Figure 55. This relationship says that for any phase of training there is an initial period over which the increase in capability per training hour is very rapid. But after that point the capability increase per hour decreases and can only be increased by changing the type or training or its environment. In fact, in combat the initial performance may decrease because of the changed environment.

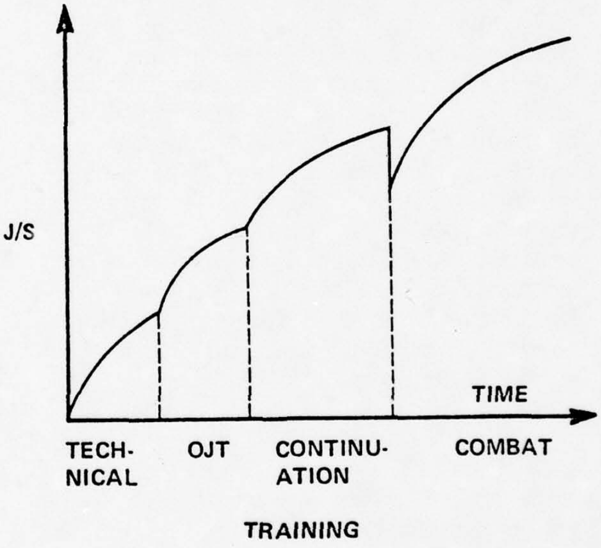


FIGURE 55. THE EFFECT OF TRAINING

[21] The maximum input data rate of a man is about 100 bits per second, and his maximum output rate is about 10 bits per second.

As an example, a very effective tactic is emission control, often called EMCON. ECM cannot be effectively deployed against a radar that does not reveal its presence. If a SAM radar is turned off, it has no sensing capability so that an OJT operator may be unable to complete an intercept when the radar is turned back on. But a combat-veteran operator may leave the radar off until the aircraft is well within firing range and yet successfully complete the intercept. Turning the radar on and firing the missile as quickly as possible gives the ECM minimum time to respond to the threat, thus the well-trained operator has retained his capability while putting the attacker at a disadvantage.

In conclusion, it is clear that both the ECM operator and the ECCM operator are working with complex equipment in a complex and fluid battle situation. A breakthrough on either side must be countered if this technical advantage is to be offset. Thus electronic warfare is fought as much in the intelligence shop and on the design boards as in the combat zone. If the intelligence and design battle has been successfully fought, so that the equipment capability is evenly matched, then the outcome depends upon the ECM and ECCM operators—their individual training and proficiency may be the deciding factors.

Chapter 7

COMMUNICATIONS

The second major military use of radiated electromagnetic energy is for communication, the sending of messages from one element of the force to another. The potential volume of communication can be enormous as Table 20 indicates. Not all these circuits will be in use at any one time; but the percentage of circuits used can be expected to increase as the urgency of the military situation increases, and this has implications for electronic warfare.

Table 20

Available Radio Communications Channels

Band	Frequency	Number of Channels
HF	3– 30 MHz	3000
VHF	112–135 MHz	2300
UHF	225–400 MHz	1750

The previous statement is deceptive, however, since it considers all the channels to be allocated only to military use. But in the HF band the available allocations are shared between military and civilian users so that the number of available military channels is much less. On the other hand, Table 20 also ignores the large volume of telephonic and telegraphic communication which often is transmitted by radio relay. In fact, it is safe to say that potentially every long distance military communication will be carried over part of its path by electromagnetic radiation.

Communications and the Electromagnetic Conflict

The relationship of electronic warfare to communications is more complex than to other uses of electromagnetic radiation because of the nature of communications itself. Military communications, although they may be about the enemy, are intended for a friendly recipient and both the presence of the message and its content are intended to be privy to the sender and receiver. It can be presumed that the enemy knows the existence of the communications channel and of the modulation techniques used to transmit and receive the message. Hence, additional methods must be used to assure message security.

In electronic warfare it is common practice to differentiate between actions directed only at the transmission of the communications signal and those that are directed at the message content. Determining the presence of a (communications) transmission is ELINT, interfering with a communications transmission is ECM and protecting a communications transmission is called either ECCM or transmission security (TRANSEC). Activities whose goal is determining the enemy message are called communications intelligence (COMINT), while communications security (COMSEC) encompasses all activities designed to protect the contents of our messages during transmission. Both COMINT and COMSEC involve *cryptology*, the science of secret communication. The analog of ECM with respect to the message is *intrusion*, the insertion of false messages into enemy communications nets. Because intrusion is difficult, it is not often attempted; conversely, when intrusion is successful substantial disruption of military effort can be achieved.[1],[2] The potential damage from

[1] Sir William James, *The Codebreakers of Room 40* (New York: St. Martin's Press, 1956). This book records several instances where Sir William Hall attempted intrusion in written communications with varying degrees of success.

[2] Paul Leverkuehn, *German Military Intelligence* (New York: Frederick A. Praeger, 1954), pp 113-116, 182-183.

intrusion makes *authentication*, the establishing of the genuineness of the sender and receiver, an important part of COMSEC.

The concepts of electronic warfare discussed previously apply equally well to communications signals. But not all messages are of the same value to an unauthorized listener, thus messages are classed in different categories of protection. Those that are most sensitive are encrypted to prevent the content of the message from being known even if it is intercepted; those that are less sensitive may be sent "in the clear" because their value to the enemy upon interception is small. In principle, COMINT does not distinguish between the categories of the messages intercepted since the sophistication of the encryption may not be apparent until decryption is attempted. Thus the essential difference between COMINT and ELINT is the additional processing applied to the received signal in an attempt to recover the message.

One process of deriving information from messages, commonly called *traffic analysis*, considers the received messages in terms of their volume and point of origination. (Since reception is a passive function, the destination of a message can only be determined from the message itself.) One facet of traffic analysis proceeds from the knowledge that the military chain of command dictates that messages originate from military headquarters of various echelons. Thus, by locating the transmitters originating the messages we have located the corresponding headquarters. With appropriate equipment this can be done at reasonably long distances without the enemy being aware of our activity; hence we gain information about his order of battle at small risk. The other part of traffic analysis considers the volume of messages sent. If the volume rises suddenly then the increased activity can indicate impending attack.[3]

The value of both items of information arises largely from the fact that the enemy is ignorant of our possession, consequently he may be lulled into a false sense of security. For such reason, such intelligence is very well protected. If we were to employ ECM to deny the enemy the use of his communications, he would become wary, and seek both to protect his messages by encryption and to change his operating practices to make the signals more inaccessible. Therefore, ECM tends not to be used against communications signals except in the heat of battle against the lowest priority tactical communications where the resultant confusion is the primary objective. For example, it is more profitable for a bomber to jam (than to listen to) the ground-to-air communications between an enemy interceptor and his ground controller since the bomber's location is already known, but the confusion caused by the jamming may prevent a successful intercept.

As we indicated previously the peculiar emphasis of communications intelligence is understanding the content of a message. Because the usefulness of this knowledge arises principally from the enemy's ignorance of our knowledge, all information about COMINT tends to be tightly controlled. However, some historical information is available which indicates its importance.[4] In addition, the general principle of cryptology have been published in the open literature so that we can gain an understanding of how messages can be protected. On the basis of this background it is easy to see the importance of *communications security*, the protecting of our own messages from foreign interception.

Cryptology and History

Because the ability to read another's secret messages has an air of romanticism about it, it is easy to distort reports of such activities to assume an importance much greater than they

[3] Price, *Instruments of Darkness*, pp 153-154 records that the Germans gained warning of attack by monitoring the frequency of aircraft maintenance radio checks.

[4] David Kahn, *The Codebreakers* (New York: Macmillan, 1967), pp 460-461.

really posses. That cryptology does posses the ingredients for a good story is attested by Edgar Allen Poe's "The Gold Bug". But more historical is the fact that the execution of Mary, Queen of Scots, in 1587 was due in large part to the decipherment of messages between her and others plotting the assassination of the Queen of England.[5] The Huguenot bastion of La Rochelle was captured by Cardinal Richelieu in 1628 in sight of the relieving English fleet in part due to the ability of the French to read the city's enciphered messages.[6] And a chief exhibit in the treason trial of Aaron Burr in 1807 was an enciphered letter.[7] Finally, in the Civil War the decipherment of messages led to the Union capture of plates for the printing of Confederate money.[8]

But all these examples occured before the advent of radio communications. To find what cryptology combined with radio communication is capable of we must turn to the First World War and subsequent history. The entry of the United States into WW I was precipitated by the public disclosure of the Zimmerman telegram, a message between the German Foreign Minister, Arthur Zimmerman, and the German Ambassador to the United States, Count Bernstorff. Although the origin of the message was concealed at the time, it was originally deciphered by the British from an intercepted telegram.[9] Later in the War, in 1918, the French "broke" the German ADFGVX field cipher used for radio communications between army units, and with the help of those messages were able to halt the march on Paris.

The American effort in COMINT and cryptology during WW I may not have achieved as dramatic successes as the Europeans, who had a longer history of interest in this field, but it did have an impact. In the field the effort was characterized by quantity production of codebooks and pamphlets for the protection of our own messages, more than 80,000 being published and distributed in one 10 month period. We also established a Security Service to monitor American radio messages to detect violations of message security practices.[10] On the home front Herbert Yardley took charge of MI-8, the cryptology section of the Military Intelligence Division, whose most important effort resulted in the conviction of the only German spy condemned to death in the United States in WW I, Lothar Witzke.[11] After the war Yardley formed the American Black Chamber, a clandestine unit of the state department. It specialized in deciphering diplomatic codes, especially the Japanese with whom we were involved in disarmament negotiations in 1921. The American Black Chamber flourished until 1928 when it was disbanded by Henry L. Stimson, Hoover's Secretary of State, acting on the principle "Gentlemen do not read each other's mail."[12] This apparent setback did much to popularize cryptology, for Yardley first serialized his experiences and then published them in a book, *The American Black Chamber.*[13]

During the depression the American cryptanalytic ability slowly developed under the tutelage of William Friedman in the Office of the Chief Signal Officer of the Army.[14] Friedman is undoubtedly the father of American cryptology, for he placed the science on a firm mathematical basis; thus paving the way for much of the extensive effort in that field today. In addition, he supervised the analysis of the Japanese

[5] *Ibid.*, pp 121-123.

[6] *Ibid.*, p 157.

[7] *Ibid.*, p 220.

[8] *Ibid.*, pp 282-297.

[9] *Ibid.*, pp 340-347.

[10] *Ibid.*, pp 330-331.

[11] *Ibid.*, pp 353-354.

[12] *Ibid.*, pp 359-360.

[13] *Ibid.*, p 361.

[14] *Ibid.*, p 385.

PURPLE diplomatic code. As a result, when the Japanese ambassadors delivered their final note to Secretary of State Hull 55 minutes after Pearl Harbor, the secretary only made a pretense of glancing through the note for he had read it already.[15]

This extensive theoretical development was not matched by a practical competence in things cryptographic on the part of the United States at the beginning of WW II. The Navy and the Army had reasonably secure codes, but the State Department's codes were so insecure that some ambassadors felt that they had been broken by all the totalitarian powers.[16] This insecurity resulted both from the antiquated codes in use and the lax security at our embassies here and abroad. As a result, much of Rommel's success early in his North African campaigns, success which earned him the title of the "Desert Fox", came from intercepts of the messages of the American military attache in Cairo, Colonel Fellers. Colonel Fellers was a meticulous man who reported to Washington in voluminous detail the dispositions of the British forces, their tactics and their problems. The Axis powers had a copy of the American Code book, the BLACK code, and turned this information into strategic intelligence which enabled Rommel to anticipate most of the British moves. Fellers was recalled to Washington about the time Rommel crossed the Egyptian border and the Americans began to use a new cipher. Hence he was not forewarned of the British plan for the Battle of Alamein which started the long German retreat in Africa.[17]

The climax of the Battle of the Atlantic occurred in March 1943 when German U-boats sank 23 ships totaling 141,000 tons in three days. The German success was a direct reflection of their ability to routinely read our convoy reports. It almost forced the abandonment of the convoy system.[18] Yet one year later, when the Allies were able to routinely read the U-boat communications, we were sinking almost one U-boat a day and as a result we won the U-boat war.[19] And in the air, the intercept and decryption of a short Allied message on the morning of August 1, 1943 gave the defenders of Ploesti several hours warning of the raid in which we lost almost 1/3 of our force.[20]

Communications Security

One should not infer from these examples that COMINT is always decisive, but that it can be potentially decisive. The volume of radio traffic is extremely large, so that there is always a chance that a certain message will go undetected; but in the examples given that did not happen. How do we prevent our messages from being read? That is the subject of communications security, the counterpart of ECCM for noncommunications signals.

Communications security has two parts, the first is operating practices which deny the enemy access to our messages and to our communications channels, and the second is cryptologic methods of protecting our messages when he does get possession of them. The operating practices are mainly common sense. For example, if the location of a particular aircraft in flight must be concealed then *radio silence* is imposed. In general, only essential messages should be sent and these should be as short as possible. *Call signs* should be used to conceal the identity of the stations and these should be changed periodically since traffic analysis will be able to associate call signs with units given sufficient time. Frequency changes and operating time changes should occur at irregular intervals. Operators should also be changed, if possible, since a Morse operator, for example, can often be identified by his "fist", his manner of sending. Finally, "passwords" or authenticator groups should be inserted into messages so that both the

[15] *Ibid.*, pp 62-63. The movie "Tora, Tora, Tora!" also portrays some of the cryptographic effort of that period.

[16] *Ibid.*, pp 493-494.

[17] *Ibid.*, pp 473-477.

[18] *Ibid.*, p 468.

[19] *Ibid.*, pp 503-507.

[20] *Ibid.*, p 464.

sending station and the receiving station can assure each other of their identities, and these should be changed periodically. The general principle is to introduce as many changes into the operation as possible so that the enemy is never certain of what he is listening to.

But operating procedures can only do so much; if we must communicate by radio then we are going to have to go on the air. So we must assume that the enemy will receive our messages also, consequently we must send them in such a form that even when he receives them he cannot understand them. This is the whole object of cryptology.

Cryptology

Cryptology has customarily been applied to written or telegraphic communication. As it is applied to radio communication it uses the following principle techniques:

Substitution
Transposition
Code Books
One-Time Pads

We shall discuss each technique briefly.

Substitution. This is probably the best known method of cryptology; many schoolboys have written secret messages with the aid of their Captain Midnight rings. In this method some other symbol is substituted for each letter of the message. For radio communications the substituted symbol is some other letter of the alphabet, but for written communications any other symbol will do. For ease in making the substitution one usually makes up a table of the equivalents. The equivalents could be assigned at random but this makes both remembering the table and changing the table difficult so a *keyword* is often employed. That is, the keyword is written down first, omitting all duplicated letters, and then the rest of the alphabet is filled in afterwards. If we call the original message the *plaintext* and the encrypted message the *ciphertext*, and if we use THUNDERBIRD as the keyword we have the following substitution table of Table 21. Suppose the plaintext is "The targets for tomorrow are a bridge and the Kep steel plant"; the ciphertext becomes "QBD QTORDQP EKO QKGKOOKW TOD T HOINRD TJN QBD CDL PQDDF LFTJQ".

This encrypted message suffers from a number of deficiencies. First we note that the word divisions are given. Now an elementary knowledge of English is sufficient for a cryptanalyst to realize that "a" is the only single letter word in common use in the language. Thus he can establish that a equals T. Next TOD and TJN become candidates for "and", and the repeated QBD is a candidate for "the". Likewise the ciphertext QKGKOOKW, with its repeated OO and three K's might be guessed to be "tommorrow" and this would fit well with QBD equals "the" and TOD equals "and". It is easy to see that only a little effort with this method, called *anagramming* would be sufficient to recover the message and the key, thus any other message in this key could be deciphered.

One way of hindering anagramming is to write the message in standard blocks like this: QBDQT ORDQP EKOQK GKOOK WTODT HOINR DTJNQ BDCDL PQDDF LFTJQ. Now the analyst would count the number of letters in the message and compare the count with the frequency of letters in the English language.[21] From this analysis (Table 22) he

Table 21

Keyword Monoalphabetic Substitution

Plaintext letters	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext letters	T	H	U	N	D	E	R	B	I	A	C	F	G	J	K	L	M	O	P	Q	S	V	W	X	Y	Z

[21] *Ibid.*, p 100.

Table 22

Frequency Analysis

Message count	0	2	1	8	1	2	2	1	1	2	4	2	0	2	6	2	7	2	0	5	0	0	1	0	0	0
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
English Frequency (%)	8	1½	3	4	13	2	1½	6	6½	½	½	3½	3	7	8	2	¼	6½	6	9	3	1	1½	½	2	¼

NOTE: English frequency percentages are taken from Kahn, *The Codebreakers*, p 100.

would then make the tentative identifications D equals e, Q equals t, T equals o, O equals a, and K equals n and then check these by anagramming. This is the same method used in Edgar Allen Poe's *The Gold Bug* and is effective on any monoalphabetic substitution cipher.

There are two methods of improving the monoalphabetic substitution. If the message must remain secure for only a short time we might use a *checkerboard substitution* such as the German ADFGVX field cipher (Table 23). The 6 letters were chosen to have distinctive Morse signals and each letter was encrypted by its coordinates. With the checkerboard illustrated the message becomes XGGVX AXGDG VXXXX AXGGD AVADV XXGAD DAADV XVXAD FDDGV XXADG VGVXG FFXXX XADGF AFXXG GVXAD DXAVA GDXGX AXAFF VAFFD GFAXG. Notice that the message is doubled in length, a disadvantage of this method. The restricted number of symbols might also suggest a checkerboard to the experienced cryptanalyst. It is interesting to note that this cipher was broken only on days when a large amount of traffic was passed over the radio.

Table 23

ADFGVX Checkerboard

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	L	0	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

The initial decipherment by the French was made with two intercepted messages which differed in length by only two letters. The analyst, Painvin, assumed that these were identical messages which differed only in the internal address.[22] This illustrates that sending identical messages, or messages with identical parts (beginnings, endings, etc.) can be a great help to the cryptanalyst. One common cause for such a practice is the occurrence of mistakes in encrypting, transmission, or decrypting. If the message does not make sense to the recipient, then he may ask for a repeat and the analyst has the second copy he wants.

The second method of improving the monoalphabetic substitution is to use more than one table—a polyalphabetic substitution. Table 24 illustrates one form of such a system, the Vigenere tableau.

We may use this tableau in two ways. The first uses the keyword to indicate which line of the tableau we are to use for encrypting each letter. The results are given in Table 25. The second merely advances one line for each

[22] *Ibid*., p 345.

Table 24

The Vigenere Tableau

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 25

Keyword Polyalphabetic Substitution

Keyword	THUND	ERBIR	DTHUN	DERBI	RDTHU	NDERB	IRDTH	UNDER	BIRDT	HUNDE
Plaintext	theta	rgets	forto	morro	warea	bridg	eandt	hekep	steel	piant
Ciphertext	MOYGD	VXFBJ	IHYNB	PSISW	NDKLU	OUMUH	MRQXA	BRNIG	TBVHE	WFNQX

Table 26

Progressive Key Substitution

Plaintext	theta	rgets	forto	morro	warea	bridg	eandt	hekep	steel	plant
Ciphertext	TIGWE	WMLAB	PZDGC	BEIJH	QVNBY	ARJFJ	IFTKB	QOVQC	GIUVD	IFVJQ

successive letter, i.e. it uses the alphabet as its keyword. This technique is often called the *progressive* key and it is preferable to the keyword in that it exhausts all the available cipher alphabets before any are used again. In the progressive key the message becomes the ciphertext of Table 26. Because the progressive key uses all the alphabets it is the more secure system.

It should be obvious that substitution keys are easily mechanized because one need merely change the electrical interconnections between keys and type bars on an electric typewriter. This is the basic idea of the rotor machine, sometimes called the Hebern mechanism, the Enigma, or the Hagelin mechanism. These machines can be built in the size of a portable typewriter with the capability that the sequence of alphabets repeats only after more than two million plaintext letters. Such a machine can be purchased on the commercial market for under $1,000.[23]

The problem of breaking such a code involves determining the period of repetition of the sequence of alphabets. This can only be done by obtaining a large quantity of text, assuming various periods, and then testing the portions of the ciphertext which are encoded by the same alphabet for monoalphabeticity with a test called the kappa test. The amount of labor is prodigious and is best done on a digital computer. However, the breaking of the Japanese PURPLE code before WW II involved just such a process, for the code was produced by a rotor machine, and all the labor of analysis was done by hand.

Transposition. Transposition is the second form of encryption, which involves interchanging the order of the letters of a message. A simple example is Table 27; the columns of a 5 x 10 matrix are numbered in arbitrary order and the message is written into the matrix row by row. The columns are then read out in order, *viz*. AOATL HOAAT RMBHP TTEDE TFWES SOGPT ERRNE ERIKA GOREL TRDEN.

This technique can be repeated as many times as desired. Transposition is inherently less flexible than substitution but it does have two important uses. One is to scramble the alphabet in a monoalphabetic substitution, thus producing a much more randomized alphabet by an easily remembered format. A similar technique was used by the convicted Russian spy, Rudolph Abel.[24] The second use of transposition is to scramble the results of a mono- or polyalphabetic substitution, thus making the cryptanalysis harder. In this use it is called a *superencipherment.*

Table 27

A Transposition Cipher

5	2	7	4	1	3	9	8	10	6
t	h	e	t	a	r	g	e	t	s
f	o	r	t	o	m	o	r	r	o
w	a	r	e	a	b	r	i	d	g
e	a	n	d	t	h	e	k	e	p
s	t	e	e	l	p	l	a	n	t

Code Books. Encryption with code books is really another form of substitution in which the substituted elements are words or phrases rather than letters. One form of the code book is a dictionary. The word is found in the dictionary and encrypted by replacing it with its page number and line number. (This is the code Aaron Burr used.) One can also use a book but the location of the words of the text when encrypting is more difficult. Dictionary or book codes for military use suffer from the fact that some of the words to be encrypted may not exist in the edition used. Furthermore, from the cryptanalytic point of view they are deficient in that the words and their ciphers are ordered identically. For example, if we encrypted the message used above in a dictionary code using Webster's Seventh New Collegiate Dictionary, 1965 Edition by the G & C Merriman Company we would get: 914213 902204

[23] *Ibid.*, p 433.

[24] David Kahn, *Two Soviet Spy Ciphers* (New York: American Cryptogram Association, 1960).

325240 930244 047107 000101 104230 033220 915101 462111 1045434 1044238 1047219 858105 647231. In this code the last two digits are the line number, the column number is the third from the end and the remaining digits are the page number.

The cryptanalyst would suspect that alphabetically the fourth word falls between the first two and if he knows one or both he may be able to guess at the other. Note also the Kep does not occur in the dictionary so that it must be spelled out. In this case the letters were taken from a separate list of abbreviations so that the ordering is broken up. However, the page number is such that those letters have seven digit codes while all the rest have six. The word "the" has been coded two different ways, there happening to be two different definitions in the dictionary. This use of different symbols for the same word, or *homophones*, conceals word repetitions from the analyst and makes his task harder.

The best type of book code for military coding is the *two-table book code*. In this the numbers are assigned randomly to words with provision made for homophones and *nulls*, code groups that mean nothing but which are inserted to confuse the cryptanalyst.[25] For example, a portion of the A. E. F.'s HUDSON code is given in Figure 56. (It was the publication of code books which accounted for the large volume published during WW I by our forces, a volume which has certainly not decreased with time.) The major problem with code books is publication, distribution and security. Code books must be changed periodically because after enough traffic has used one edition it is quite probable that the enemy has been able to reproduce it, if not through cryptanalysis then by the "practical" technique of theft.

One-Time Pad. The last major technique, the one-time pad, is really a form of substitution with the distinction that the particular cipher key is used only once. Rudolph Abel used several, and their recovery further implicated him as a spy; since no ordinary citizen would have a use for them.[26] The one-time pad idea can also be applied to teletype. Special teletype machines are available which accept two tapes, a message tape and a key tape. The resulting output is the combination of the consecutive symbols on the two tapes. If the key tape is unique, then the result is a one-time pad. Incidentally, this is

ENCODING	
STOP	3514
STOPPED	3329 – 4017
STORM	4211
STRENGTH	1740 – 2329
STRENGTH OF ENEMY UNKNOWN	3961
STRENGTHEN	1679
STRETCHER BEARERS	3166
STRIKE	5056
STRIP	3515
STRONG	3141
SUB	5639
SUCCEED	3237
SUCCESS	1790

NULLS:
2089
4286
2094
2553
2399

DECODING	
1629	NON
1630	6-INCH
1631	'S
1633	A
1636	WAS
1638	DOES NOT
1640	WILL BE
1644	BENGAL FLARES
1645	OUR WIRE
1646	AND
1647	-IED
1648	DARKNESS
1651	UNIT

FIGURE 56. AN EXTRACT OF THE A.E.F.'S HUDSON CODE (ADAPTED FROM, THE CODEBREAKERS, **P 328)**

[25] Kahn, *The Codebreakers*, p xiv.

[26] *Ibid.*, p 664.

the method used to assume privacy for the Washington-Moscow hot line. Both the teletype machines and the key tapes are procured commercially.[27]

It is interesting to inquire what is the magnitude of the job of supplying keys for a teletype link. If we have a 100 wpm (words per minute) teletype running continuously—so that beginning and endings of messages cannot be determined by an analyst—then we are sending about 500 characters a minute or 720,000 characters a day. A rotor machine with a non-repeating sequence length of 2 million would repeat itself every 3 days. Thus the requirements for keys can be severe.

Table 28

Cryptographic System Comparison

	Difficulty[1]	Security		
System	of use	Level[2]	Duration[3]	Support[4]
Substitution				
Monoalphabetic	Low	Low	Short	Low
Checkerboard	Low	Moderate	Moderate	Moderate
Polyalphabetic				
Keyword	Moderate	Moderate	Moderate	Low
Progressive	Moderate	High	Moderate	Low
Transposition				
Simple	Low	Low	Short	Low
Superencipherment	Moderate	High	Long	Moderate
Code Book	Moderate	High	Long	High
One Time Pad	Low	Very High	Very Long	Very High

[1] In terms of the communicator who must use the system.

[2] The susceptability of the system to cryptanalysis.

[3] The length of time any one key can give protection. Obviously protection is increased by changing keys and decreases as the volume of traffic encrypted by a particular key increases.

[4] The amount of material that must be distributed to employ a particular system and/or the coordination that must be employed for a particular system to be used.

From the above discussion, it should be clear that the communicator has a wide choice of cryptographic techniques especially when one considers the combinations available. The one used will depend on the priority of the message and the degree of security

[27] *Ibid.*, pp 715-716.

desired. Table 28 summarizes the characteristics of the four major systems.

Speech Encryption

We have talked almost exclusively about teletype, how would one encrypt voice? There are five possible methods. One method is to divide the frequency spectrum of voice into several parts and rearrange the parts. However, this system is relatively insecure, both because spectral analysis can recover the transposition and because a listener with some training may be able to understand the scrambled version, especially if the transposition is not well done.[28] This results from the great redundancy of speech, as reflected by the fact that its spectrum is more than 10 times that needed to transmit the information content. Thus the human ear need recognize only a few characteristics to interpret the sounds.

A second method, called time-division scramble or T.D.S. for short, chops the speech into short segments which are then transposed in order and sent.[29] A third method would be to sample and quantize the speech, that is to approximate the amplitude of the samples with fixed increments. The quantized amplitudes could then be converted into numbers which could be encrypted by any means, such as a polyalphabetic substitution cipher. Such a procedure is very similar to the technique of pulse code modulation. Its disadvantage is that it requires much more bandwidth than speech itself.

The fourth method is that used during the Second World War, one encrypts language with language; that is, one uses speakers whose language is understood only by our forces. During the war several units used American Indians, whose languages were not understood by the enemy, as their radiomen to permit secure communication.[30] Finally, one may seek to eliminate the redundancy from voice through a special type of machine called a vocoder. This machine extracts the basic vocal parameters forming speech, which parameters vary at rate approximating the information content of speech. By suitably encoding these parameters and sending them one could cause a similar machine at the other end to emit synthetic speech.

One of the basic problems with making voice communications systems secure by mechanical or electronic means is that the symbol rate is much faster than for teletype. Since the only reason for making a voice system secure is to preserve the immediacy of speech and thus gain the advantage of rapid communication, one must encrypt the system at this faster symbol rate. If one uses a one-time pad encrypting scheme, a speech system will require a greater quantity of key tapes than a teletype system. For example using a vocoder to eliminate redundancy will make the symbol rate about 10 times that of the teletype; but digitizing the speech directly may make the symbol rate as much as 30,000 times greater. For this reason, and because speech is more difficult to disguise, teletypewriter systems are preferred for maximum security.

Authentication .

Although the preceding material is usually implied by the term communications security, yet it must be recognized that authentication is also an essential part of this area. For even if our messages are completely secure cryptologically, if the intended recipient never receives them the enemy has achieved an important advantage.

One reason why authentication is easily overlooked is that in much private and commercial communication authentication is inherent in the message. We "recognize" the voice on the telephone, the address on the letter, the handwriting of the letter or the signature, the style of the writer or the phrasing of the speaker, or the message makes reference to information which only the correct originator would have known. In fact, one of the important design parameters of the telephone system is that sufficient fidelity be

[28] *Ibid.*, p 558.

[29] *Ibid.*, p 554.

[30] *Ibid.*, pp 549-550.

introduced so that this authentication is easily done. On the other hand, a common strategem in the "who-done-it" is the muffled voice on the telephone, and no spy thriller is complete without a password or two.

Thus authentication is a common aspect of communication, but it has not received much emphasis in the communications literature because it is so self-evident. And one would not expect much open military or governmental mention because the authenticator procedures clearly must be well protected. But the recent advent of computer data files and the clear need for insuring data privacy has raised the twin issues of crytopgraphic security and authentication in that field.[31] And from the unique problems of the commercial computer world we can learn something about both areas.

First, we must recognize that the form of the message influences strongly the suitability of the security system. The messages we have discussed are those using language, which has a high degree of redundancy.[32] The strongest cryptologic systems (substitution with superencipherment and the one-time pad) have tried to make each letter secure independently of any other letter. The other two systems, transposition and code-books, attempt to randomize the inherent message redundancy because that redundancy is a great asset to the cryptanalysist. Together the two types, individual letter security plus randomizing the redundancy have provided the possibility of impregnable codes.

Now if the communication system is perfect these security systems are more than adequate, but what happens if the message is received with transmission errors? In the traditional systems, with their independent symbol protection, only a single letter is affected, and the message is still intelligible because the erroneous letter can be inferred from the rest of the message. Even with the code book, which has the least redundancy implied by grammar and syntax, the remaining redundancy will help reduce errors. Hence these communication systems, including handwriting, have been adequate in the past even though they are prone to errors.

But for direct computer-to-computer communication the messages are commonly digit streams with very little redundancy. Now if an error creeps in, a large portion of the message may be wrong, or unintelligible, or both. With the increasing use of computer technology by the military, this problem will have to be considered by the military commander also.

The reason for digressing to cryptologic systems here is to emphasize that conventional authentication procedures rely heavily on subtle factors contained in the message redundancy structure. When these factors are absent additional redundant symbols (in the sense that they do not contain any message information) must be added to authenticate. However, it is also common practice to add redundancy to detect and prevent transmission errors.[33] Thus it appears that we might be able to use the deliberately added redundancy for authentication as well as for error detection and prevention.

In fact, one of the proposals for computer privacy does exactly that.[34] It uses a polyalphabetic system for encryption, but added to this system are "diffusion" operations which increase the intersymbol dependency, or redundancy, of the message. Each sender has a "password" or authenticator which is used also as a keyword for the encryption process, the resulting encryption is sufficient to both protect and authenticate the message. For if the message and sender are genuine and the transmission perfect then the message is intelligible and authenticated, otherwise the message is hopelessly garbled and is rejected.

In summary, authentication must be considered as potentially important as message cryptographic security in communications security. In the past, the two

[31] Horst Feistel, "Cryptography and Computer Privacy", *Scientific American*, 228 (May 1973); p 15.

[32] Any book on information theory will define redundancy. John R. Pierce, *Symbols, Signals, and Noise* (New York: Harper & Row, 1961), is a fascinating book on information theory written for the layman.

[33] This is done through error detection and correction codes.

[34] Feistel, "Cryptography and Computer Privacy", p 23.

concepts have been treated separately because the high message redundancy predisposed to cryptologic systems with no redundancy. Thus authentication with its added redundancy became a transmission function divorced from the message originator. But with the advent of high-speed, non-redundant digital transmission, additional redundancy must be added to eliminate transmission errors. Thus there is the potential for turning the redundancy adding process into a means for incorporating authentication also.

Chapter 8

FUTURE REGIONS OF THE ELECTROMAGNETIC CONFLICT

The previous seven chapters represent the classical approach to electronic warfare, if a field with so short an history can be said to have a classical approach. But the technological advances of the last 30 years have expanded the use of electronics in warfare, consequently the areas of application of electronic warfare have also expanded. In many of these areas electronic warfare is not fully developed, neverthless we want to survey the new areas, indicating some of the potential uses and some of the possible EW applications.

Because these topics are somewhat of a potpourri, we will not be able to make a clean division of topics. However, we have chosen three general areas to discuss: sub-centimetric technology (millimeter waves, optical and infrared wavelengths), unintentional radiation and "smart" weapons.

Sub-Centimetric Technology

Because electronic warfare is based on electrical technology it is not surprising that the traditional concepts have been formulated in terms of radiation of metric wavelengths and longer, for this was the technology of the Second World War when electronic warfare was born. However, the turn of technology to shorter and shorter wavelengths has brought about changes in capability which must be accounted for in our electronic warfare concepts. For example, as the wavelength becomes shorter, the resolution capability of a radar becomes progressively better. Thus an effective jamming or deception technique which halves the resolution of a 100 MHz radar may not be effective against a 100 GHz radar even though it also halves the resolution. The reason is that the typical 1/2 mile (1 kilometer) resolution of the low frequency radar is much larger than the target and barely adequate without jamming. The high frequency radar, on the other hand, could have an effective resolution of 3 feet (1 meter) which is much smaller than the target and more than adequate for its task. Thus a similar ECM technique would be ineffective even if it achieved the same degradation.

As this example implies, subcentimetric technology is characterized by electromagnetic radiation whose spatial wavelength is of the order of centimeters or less. In our discussion, sub-centrimetric will mean signals with frequencies greater than 10 GHz. This region naturally divides itself into millimetric waves (10-1000 GHz), infrared (1–400 THz),[1] and optical wavelengths (400–800 THz). The latter two divisions are naturally occurring phenomena, we classify them as technologies because it is our emerging capability to electronically convert radiation in these bands to electrical energy and vice versa that makes them useful militarily. Thus our initial discussion of their properties will be an expansion of the discussion in Chapter 2 concerning electronic threats. But we also want to indicate some of their electronic warfare potential as we proceed.

Millimetric Waves. The area of the millimetric waves is really the area of the frontier in radio frequency research. Concerning airborne users, the real attraction of this frequency range is the small component sizes required because of the small wavelengths (Figure 57).[2] Since small size typically means light weight, airborne users are doubly interested in this technology.

A corresponding benefit of these frequencies is the increased resolution possible because of the smaller wavelengths. For example, we consider the "pictures" (displays) produced by conventional radar very fuzzy because our eyes respond to the

[1] THz is the abbreviation for Terahertz, 10^{12} hertz. See the Glossary under "Unit Prefixes."

[2] Data for Figure 57 is derived from Skolnik, *Radar Handbook*, Chapter 9, p 5 and Chapter 10, p 10.

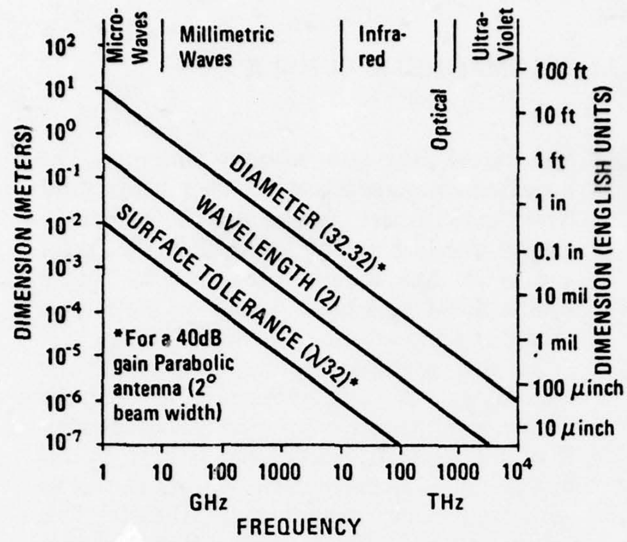


FIGURE 57. SUB-CENTIMETRIC TECHNOLOGY

very high resolution optical wavelengths, where the dimensions of typical objects are of the order of several wavelengths, rather than fractions of a wavelength. Thus, increasing frequency means that we can obtain a more "realistic" portrayal of a target. A case in point is an airport surface detection radar operating between 10 and 20 GHz which allows the operator to distinguish between different aircraft because he can count the number of engines, etc. Thus in a military context the better resolution would greatly simplify the problem of target identification.

But these wavelengths also have some disadvantages. The most important one, and the one that has greatly limited development, is again related to small size. In order to control and process the radiation, the physical structures must have transverse dimensions no larger than a wavelength. But the voltage breakdown strength of air and other insulators is independent of frequency so small size means low voltages, hence low power. This can be seen from the theoretical maximum power ratings of rectangular waveguide (Figure 58).[3] Since this or similar waveguide is commonly used to connect a transmitter to its antenna then these power ratings are reasonable approximations to the maximum expected transmitter power.

Another consequence of short wavelengths and small component size is the tolerance that must be maintained to retain the desired technical characteristics of devices. Figure 57 shows the surface tolerance of a 40 dB gain antenna. This tolerance is a constant percentage of a wavelength (3.1%) or of the antenna diameter (.01%), but above 100 GHz it is of the order of magnitude of the surface finish. Thus component fabrication becomes more difficult as the frequency increases, and maximum antenna gain (maximum beam sharpness) may be limited by manufacturing tolerances.

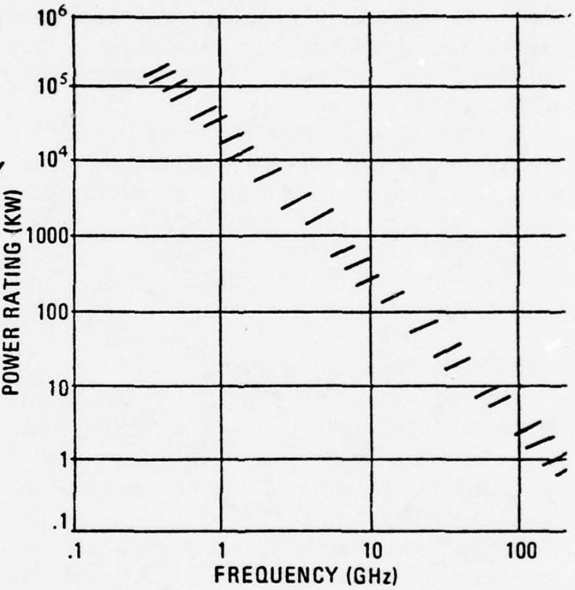


FIGURE 58. STANDARD WAVEGUIDE POWER RATINGS

Another factor limiting the use of all subcentrimetric waves is absorbtion by atmospheric gasses. Figure 59 shows the

[3] Data for Figure 58 is derived from ITT Federal Laboratories, *Reference Data for Radio Engineers, Fifth Edition* (Indianapolis, Indiana: Howard W. Sams and Co, Inc, 1970), Chapter 23, p 90.

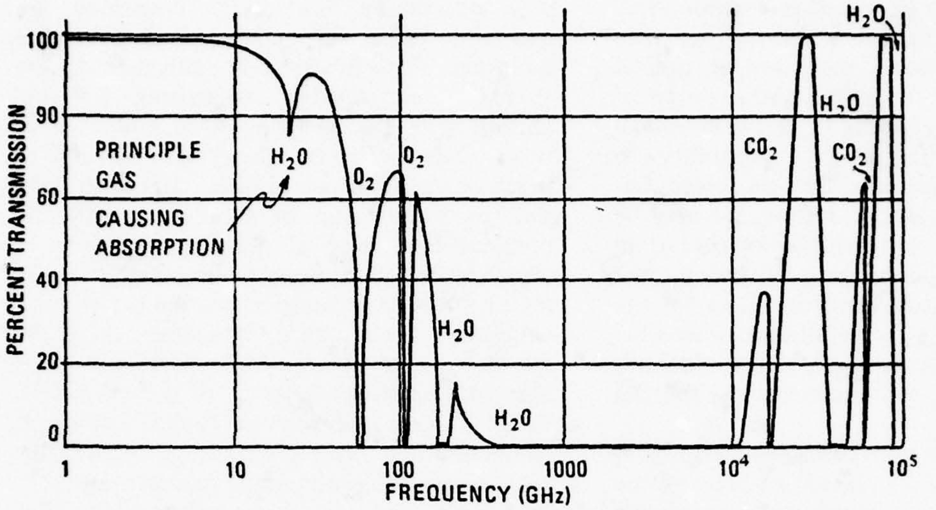


FIGURE 59. ONE-WAY TRANSMISSION THROUGH THE TROPOSPHERE AT 30° EVEVATION ANGLE

major "windows" where transmission is possible.[4,5] Above 300 GHz the high loss due to water vapor prevents employment of radiated energy until the windows in the infrared are encountered.[6] Thus millimetric wave technology in the atmosphere is limited to frequencies below 300 GHz. In addition to the atmospheric gasses, the weather phenomena of clouds, fog, rain, hail, and snow will attenuate a radiated millimetric signal. This effect becomes larger as the frequency is increased because the size of the visible precipitation becomes a larger fraction of a wavelength. Thus in the atmosphere we can expect a severe range restriction compared with more conventional radio frequency systems. However, this range restriction can be an advantage since it gives effective concealment for all but close-in surveillance. If we look to operations outside the atmosphere, in space, these propagation factors disappear and we are left with only the limitations due to low power and high fabrication cost (due to precise tolerances).

The use of millimetric radars and communications systems should be no different than those of longer wavelengths. Of course, we would expect those uses which require high-resolution, short-range radars, and high volume communictions systems to predominate. On the other hand, because these frequencies are the edge of technology, the country which deploys the first system, even though it is of low quality or capability, enjoys a technological advantage over its enemies. Thus our electronic warfare community must be continually aware of new developments in this area, in order to avoid giving a clear advantage to the enemy.

Optical Wavelengths

In contrast to the submillimetric waves, optical wavelengths have been used for centuries in weaponry, since they are the radiation the human eye senses. Even for precision weapon guidance the optical sight is acknowledged to be very accurate, its limitations come many times from the limited capabilities of the human operator. What gives

[4] Data for Figure 59 is derived from the following three references: David K. Barton, *Radar System Analysis* (Englewood Cliffs, NJ: Prentice Hall, 1964), pp 469-70; J.H. Van Vleck, "The Absorption of Microwaves by Uncondensed Water Vapor" *Physical Review*, 71 (April 1, 1947): p 432, and William L. Wolfe, *Handbook of Military Infrared Technology* (Washington DC: Office of Naval Research, 1965), pp 252-254. The last book can be obtained from the Superintendent of Documents, US Government Printing Office, Washington DC.

[5] The data has been smoothed to eliminate the fine detail.

[6] D.E. Kerr, *Propagation of Short Radio Waves* (New York: McGraw-Hill Book Company, 1951), p 648. (Volume 13 of the MIT Radiation Laboratory Series).

optical wavelengths so much new potential for weaponry is the development of the laser.

The laser can be expected to provide three capabilities heretofore unavailable. First, the laser is a narrowband amplifier at optical frequencies. Thus there exists the potential for performing direct amplification at optical frequencies similarly to our capability to perform direct amplification at lower frequencies. As technology advances we may be able to make the bandwidths wider, but in any case we should be able to increase the sensitivity of optical detectors in much the same manner that a preamplifier increases the sensitivity of a microwave receiver. So both the threat and our reconnaissance capabilities may increase.

Second, as with more conventional amplifiers, if the gain is increased sufficiently the amplifier begins to oscillate and becomes a source of radio frequencies. Thus the laser can be used as an extremely powerful source of optical waves, a source that we can control.

Third, optical wavelengths allow us to do signal processing through the holographic techniques. These techniques use the long spatial and temporal coherence of laser radiation to do quickly what digital techniques take much longer to accomplish. It can be shown[7] that the essential feature that allows this speedup is that optics permit parallel processing of information in space while digital computers must process information serially in time.

Since the laser figures so heavily in our exploitation of optical frequencies it appears worthwhile to discuss its unique characteristics (as an optical source) in more detail. Following that we shall be in a position to understand why some of the optical signal processing techniques are so powerful, and what are some of their electronic warfare applications. To aid this discussion, we will refer to Table 29 which compares a ruby laser with a very familiar natural source, the sun.

Laser Characteristics. The four unique characteristics of a laser are monochromaticity, directionality, coherence, and intensity.[8] The first, *monochromaticity*, is a one-word way of saying that laser emissions are confined to a very narrow band of frequencies. Thus the laser is equivalent to the typical microwave transmitter. Monochromaticity can be specified in a number of ways. One way is to specify the stability in hertz or in parts per million, that is, to give the expected range of variation about the nominal frequency. If this figure is given in wavelengths, it is sometimes called the *line width*. An alternative specification is temporal coherence, the length of time over which the waveform can be accurately predicted given the knowledge of one cycle of the waveform. Table 30 lists stabilities of typical lasers and compares them with a microwave transmitter. It is clear that laser stabilities can be very impressive, especially when one considers that their frequencies are of the order of 100,000 times greater than the microwave oscillator.

Monochromaticity does not play any great part in producing laser effects other than improving focusing by minimizing the effects of chromatic abberration in lenses. But the resultant stability does make communications and doppler radar applications attractive. In terms of electronic warfare applications, the narrow line width potentially allows one to modulate the output in order to achieve the spectrum and waveform desired. The capability to AM, FM, and pulse modulate a laser, as well as to heterodyne (or frequency convert) and frequency multiply its output has been demonstrated in the laboratory using a variety of techniques. However, as far as is known, these techniques have not been incorporated in operational equipment, probably because the technology is not well enough developed.

The second characteristic, *directionality*, arises from the geometrical arrangement of the elements of a laser. Laser radiation is typically generated in an optical cavity containing the lasing material bounded by opposing mirrors whose spacing is typically

[7] G.W. Stroke, *An Introduction to Coherent Optics and Holography, Second Edition* (New York: Academy Press, 1969), pp 2, 88-89, and "Optical Computing" *IEEE Spectrum*, 9 (12 December 1972), pp 24-41.

[8] J. F. Ready, *Effects of High Power Laser Radiation* (New York: Academic Press, Inc, 1971), pp 17-21.

Table 29

Natural Versus Laser Radiance

Descriptor	Sun (5900°K)	Ruby Laser
Source Characteristics		
Total Power (watts)	4 x 10^{26}	10^{-3}
Area (cm^2)	6 x 10^{22} (total) 1.5 x 10^{22} (observed disk)	1
Radiant emittance[1] (watts/cm)	6870	10^{-3}
Beam Divergence[2] (Sr)	4π	2.5 x 10^{-5}
Brightness or Radiance[3] (watts/cm^2 Sr)	2200	4 x 10^{11}
Center Frequency[4]	0.49μ 348 THz	0.6943μ 432 THz
Line Width[5]	0.59μ 524 THz	10^{-4} μ 0.06 THz
Spectral Radiance [6,3] (watts/cm^2 Sr μ)	2900 max 2300 @ 0.6943 μ	4 x 10^{15}
Illumination Characteristics[7]		
Beam Spreading Angle (Sr)	2.7 x 10^{-4}	2.5 x 10^{-5}
Spectral Irradiant Flux[8,6] (watts/cm^2 μ)	0.2 max 0.15 @ 0.6943 μ	10
Irradiant Flux[8] (watts)	0.14 total 2 x 10^{-5} @ 0.6943 μ	10^{-3}
Minimum focused spot[9] (cm^2)	3 x 10^{-8} total 4 x 10^{-9} @ 0.6943 μ	4 x 10^{-9}
Maximum Focused Irradiance[8] (watts/cm)	5 x 10^6 total 5 x 10^3 @ 0.6943 μ	2.5 x 10^5

NOTE: Ruby Laser data obtained from J. F. Ready, *Effects of High Power Laser Radiation*, pp 17-21.

[1] Radiant emittance is the radiant power emitted per unit surface area.

[2] The Steradian (Sr) is the unit of solid angle. Its value is the ratio of the area of a spherical surface intercepted by a cone with vertex at the center of the sphere to the square of the radius of the sphere. There are 4π steradians in a sphere.

[3] Lamberts' Cosine Law is assumed to hold for the sun.

[4] The frequency or wavelength of maximum radiant energy emission. For the laser the frequency and wavelength are equivalent; for the sun they are not equivalent because of the nature of the radiation process.

[5] The 3dB line width.

[6] The adjective "spectral" signifies a value per unit wavelength.

[7] Assuming a 1 cm^2 aperture without focusing. Note that increasing the aperture will increase the radiant flux of the sun but not of the laser.

[8] Irradiant means the radiant power impinging on an object.

[9] Assuming no lens abberations.

Table 30

Typical Signal Stabilities

Type	Maximum	High Power
Laser Gas		
CW	8 Hz	2 GHz (He-Ne) 50 MHz (CO_2)
Pulsed	—	50 MHz (CO_2)
Optically Pumped Solid Laser		
CW	62 KHz	5 MHz
Pulsed	—	$10^{-4}\mu$ $.02\mu$
Injection Laser		
CW	10 - 50 MHz	—
Pulsed	$.002\mu$	—
Microwave Oscillator		
CW	8 Hz	—
Pulsed	—	500 Hz

SOURCE: S. L. Marshall, *Laser Technology and Applications* (New York: McGraw-Hill Book Company, 1968), p 215; and Skolnik, *Radar Handbook*, Chapter 17, p 49, and *Introduction to Radar Systems*, p 143.

one thousand times the wavelength, or more. Only energy which traverses the cavity many times promotes the lasing action so that its direction of propagation must be coaxial with the centerline of the mirrors. This directionality allows all the energy to be easily gathered for use, as opposed to a non-directional source, where it is difficult to collect all the energy and direct it in a preferred direction. Thus directionality contributes to the "laser effects" by allowing us to collect all the laser output for use. This characteristic is illustrated in Table 29 where both the beam divergence of the emitted radiation and the beam spreading angle of the received radiation is much greater for the sun than for the laser.

The third characteristic, *coherence* is the distance over which the radiation field is predictable given the knowledge of one portion of the field. For a laser the light is almost perfectly coherent across the end of the lasing medium (e.g., ruby rod, gas column or semi-conductor junction) and coherent along the beam for distances between 30 and 100,000 kilometers.

Coherence contributes indirectly to laser effects because the coherence across the beam allows sharp focusing (limited only by the light wavelength) and high directionality of the beam. This is in contrast to more conventional sources which cannot be focused to a spot smaller than the source. And even the sun can be focused to the spot size given in Table 29 only because its great distance produces coherence over a 1 cm^2 aperture. Coherence allows a cw laser to be used as a distance measuring device over large distance through using interferometric techniques. Spatial coherence also permits holographic signal processing techniques, of which we will ;ay more later.

The last characteristic, *intensity*, is the one for which lasers are best known. Lasers generating powers of 60 kilowatts have been reported in the scientific journals.[9] These power levels are not unique but the combination of monochromaticity, coherence, directionality, and intensity is unique.

In order to obtain energy with the same monochromaticity, coherence and directionality as the laser, the light from most other sources must be frequency filtered by a narrow bandwidth filter and colimated and apertured to obtain coherence and directionality. In so doing, most of the power is thrown away. This is clearly seen by comparing the radiance, irrandiance, spectral radiance, and spectral irradiance of the sun and a ruby laser. Although the sun is much more powerful than the laser, yet when we consider the results per square centimeter of surface after filtering to the laser line width the laser is much brighter. More representative is perhaps the maximum incident power which can be achieved by focusing the energy on a minimum-sized spot. The sun and the laser are competitive, yet the laser has a much smaller total power.

Operational Applications. Each one of the four laser characteristics can be exploited in the electromagnetic conflict. However, successful use often depends upon the combination of characteristics available in the laser. We shall discuss three of these: optical radar, high-energy lasers, and optical signal processing.

The monochromaticity and directionality of the laser output means that optical radars are now feasible. In radar applications all the radar concepts such as cross-section, resonance, and ranging are applicable. Since the wavelengths used are the same as those sensed by the human eye optical radars are primarily used as rangefinders, because the eye is much better at obtaining panoramic views.

The primary advantages of optical radars derive from their very high frequencies. First, high gain (very highly directional) antennas can be obtained. Thus one can discriminate between two targets very close together in azimuth on the basis of antenna pointing. So the optical radar becomes a good complement to the optical sight. Second, very short pulses can be generated, on the order of picoseconds (10^{-12} seconds), because these pulses still contain many cycles of the radiation. But a picosecond pulse implies a resolution of .0005 foot or .006 inch. With a sensitive detector this implies the ability to detect small variations in surfaces or to detect the different materials used in constructing transparent structures. Third, these capabilities are obtained with a unit which is small physically and thus well suited to airborne applications.

The high-energy laser relies primarily on the coherence and directionality characteristics of the radar to produce a small, very intense spot of light. In this application, the laser becomes a weapon, with several possible applications. With the current state of the art it is possible to damage optical detectors whether they be inanimate or animate, e.g. human eyes. (The existence of rigid safety standards for scientific and commercial uses of lasers is ample testimony to this fact.) And it appears that generation of sufficient energy to cause structural damage to aircraft is within our grasp. The one major problem in these applications is that the energy must be focused in a small spot to create the high energy levels needed. If the system being attacked uses optics then the focusing is accomplished by those optics, and pointing accuracy is not critical. But structural damage applications require high pointing accuracies in order to insure that a vital spot is hit, so that the mechanism directing the weapon becomes as important as the laser itself.

The third application, signal processing, relies on the coherence and monochromaticity of the laser. Actually there are three areas of optical signal processing which have potential application in the electromagnetic

[9] Edward T. Gerry, "Gas Dynamic Laser", *IEEE Spectrum*, 7 (November 1970): 51-58.

conflict: side-looking radar, image deblurring, and correlative pattern recognition. The first area was briefly discussed in Chapter 2. The point that we want to emphasize here is that without optical signal processing techniques the side-looking radar would still be a concept, not a flying reality. The second technique, image deblurring, takes an out-of-focus or otherwise blurred photograph and restores the "original" sharpness. To date its main application appears to be scientific measurements, and its main limitation appears to be that one must know the characteristics of the blurring operation. But clearly the technique has the potential of allowing cheap photographic systems to yield high quality information.

The final area, correlative pattern recognition, has potential in many areas of countermeasures. It can be appreciated that with the proliferation of electronic equipment the number of signals in the atmosphere is increasing. One of the problems of electronic warfare is to identify the known signals, either to exclude them in a search for the unknown as in ELINT, or to permit proper action to be taken. Such a process is essentially searching a dictionary of signals to determine if the observed signal matches any of them. Optical signal processing offers the potential of speeding up this process. Hence if it can be developed (it has only been demonstrated as far as is known) there is the potential of a technological breakthrough.

Thus optical wavelengths are important not only because of weapon possibilities, but also because there may be tremendous capabilities available for signal processing to facilitate the determination of the threat and the application of electronic countermeasures against the threat. And we must not forget that optical sensors remain as some the most capable that we have, when coupled with the appropriate computation capability. What designer would not want an optical sensor with milliradian resolution mounted on a two-axis gimbled servo with good vibration isolation. Yet each of us has two of these—eyes.

Optical Noise. There is one other aspect of optical wavelengths which must be considered in signal processing applications, and which is different from that of lower wavelengths. It is the mechanism for the generation of noise. As you may remember, in the early part of Chapter 2 it was mentioned that all electronic systems are ultimately noise limited. This fact can often be ignored in electronic warfare because ECM supplies so much additional noise that the naturally occurring noise is completely overshadowed. But many of the applications of optical (and infrared) wavelengths are found in passive sensors which are designed to be as sensitive as possible, that is, they are designed to operate as close to the level of the noise as possible. And if the amount of light is minimized in signai processing then noise will also have to be considered.

At lower frequencies noise occurs as the result of random thermal motion of the charge carriers—electrons for example. The amount of noise which is produced is directly proportional to the effective temperature of the device.[10] Thus low noise devices, such as radar preamplifiers, are often cooled to reduce the noise they produce.

But basic to the quantum theory of electromagnetism originally developed by Einstein is the idea that electromagnetic radiation is produced in discrete bundles or quanta. One quanta of electromagnetic energy is called a photon, and its size is directly proportional to frequency, being equal to hf where h is Planck's constant, 6.6256 x 10^{-34} watt-sec^2. Since energy is emitted in bundles in a random fashion, then all signal generation ought to have "self-noise" as a result of the basic quantum generation process. To facilitate comparisons we can calculate the effective temperature of this self-noise by equating the noise energy per hertz, kT, with the photon energy per hertz, where k is Boltzmann's constant, 1.38054 x 10^{-23} watt-sec/°K. When the self-noise temperature is greater than the physical temperature then the self-noise or quantum noise dominates.

[10] Skolnik, *Introduction to Radar Systems*, p 23.

Carrying out the calculation indicated above we obtain

$$T_{photon} = \frac{h}{k} f = 4.79928 \times 10^{-11} f \ {}^{\circ}K \quad (16)$$

This equation shows that at the normal radar frequencies the radiation self-noise is much less than the thermal temperature so that thermal noise predominates. But at optical frequencies (above 4×10^{14} Hz or 400 THz) the equivalent temperature of the self-noise, or *quantum noise* as it is called, becomes much greater than the temperature of most devices. Thus we would expect quantum noise to dominate.

From probability theory we learn that if we have n objects arriving every second, then the rms noise associated with the process is $\sqrt{n}$. Hence the signal-to-noise ratio associated with measurement based on only a few photons will not be small. In fact, to obtain a signal-to-noise ratio of 30 dB (1,000) will require one million photons. But the one milliwatt laser of Table 30 is emitting only 3.5×10^{15} photons per second, or 8 every cycle. Now detection is often accomplished by letting the photons dislodge electrons from a suitable material, so that a perfect detector would produce only eight electrons per cycle. Thus if we attempt signal processing on a cycle-by-cycle basis, we will have a very noisy signal. If we are willing to average over 125,000 cycles we can obtain a 30 dB signal-to-noise ratio. Fortunately such an average only requires .3 nanosecond, but the result of quantum noise would probably limit any optical modulation (communication) or signal processing device based on this laser to a .001% bandwidth. Thus the bandwidth of the ruby laser of Table 29 is approximately 3 GHz in communications of signal processing applications. If the bandwidth must be increased above 3 GHz, then it could only be done by increasing laser output power. And this problem becomes worse as the frequency increases because the energy per quanta increases.

This discussion of optical noise should not be allowed to obscure the fact that all the other noise sources encountered in radar are also present. That is, there is the thermal noise associated with the electronic circuits as well as the clutter and attenuation occurring because of precipitation and clouds and because of refractive index changes in the atmosphere. In fact, optical signals may be more severely affected by atmospheric phenomena because the short wavelengths mean they are sensitive to more localized phenomena.

Infrared

The infrared frequencies are intermediary between millimetric wavelengths and the optical wavelengths. They would represent a further extension of the millimetric frequencies if it were not for the fact that the wavelength of this radiation is short enough that an orbital electron in a thermally excited atom becomes an efficient radiator. Thus infrared radiation is emitted by hot materials. This fact, in turn, means both that there is a naturally occurring background radiation level in the infrared, and that hot objects, such as aircraft engines, are natural sources of infrared energy. Of course, very-hot objects also produce optical wavelengths, but for many military uses the strongest radiation occurs in the infrared.

It was this emission of "invisible rays" that first caught the attention of Sir William Herschell in 1800. Herschel established that these rays, which were very similar to light, could be detected by a thermometer. But he also showed that there were significant differences in the ways which many materials transmit light and the rays which we now call infrared.

The next hundred years yielded more detailed information on the nature of infrared, on efficient detectors, on the properties of various materials transparent to the infrared radiation, and about the natural sources of infrared, such as the sun. In the early 1900s enough of the background had been filled in that various scientists could begin to consider the application of infrared to solve practical problems. Thus in World War I an infrared search system was developed which could detect aircraft at a distance of 1 mile.

Between the first and second World War infrared spectroscopy emerged as a key analytical technique for use by chemists. During this period the photon detector and the image converter[11] were developed. As a result of this development, World War II saw the first operational military application of infrared devices. The German Army fielded the Lichtsprecher, an infrared communication system in North Africa in 1941. They also developed an infrared fire control system for tanks which proved quite effective on their eastern front in 1944. The United States also developed infrared communications systems for Naval use, but probably the most well-known development was the sniperscope, an active, night-vision device consisting of an illuminator and an image converter. After the Second World War, infrared devices continued to be developed, with the most recent being the heat-seeking (infrared-guided) air-to-air missile, such as the Sidewinder.[12]

Since the use of infrared is relatively new in military circles, even compared to the recent advent of radar, and since it differs in some important respects from what we tend to consider as "normal" electromagnetic radiation, it seems best to discuss infrared radiation in more detail. In one sense this is an extension of Chapter 2; but since the majority of infrared signals are inadvertently radiated, they are not as much as an enemy threat as a self-inflicted threat. So we have chosen to discuss infrared separately.

We will discuss the nature of infrared (or IR) sources first. Next we shall consider IR propagation, then we shall turn to IR detectors and finally we shall discuss some military applications of infrared with their implications for electronic warfare.

Infrared Sources. Because all objects radiate infrared energy, the description of most infrared sources is not as precise as the electromagnetic sources we have been dealing with. A short reflection should show that heretofore we have described sources in terms of their frequency and their power—two numbers—and for many sources, i.e. transmitters, that description is perfectly adequate for our purposes. Some sources, such as barrage jammers, have required a power spectrum, a plot of the power output at different frequencies, but again a simple rectangular plot is an accurate enough portrayal for our purposes. But even in the latter case, the spectrum is a manufactured one, that is, we take a single frequency source and modify it (modulate it) to obtain the desired spectrum. Thus in a real sense we have complete control over the emitted spectrum.

However, for all infrared sources except the laser the above situation is not true. Every infrared source comes, as it were, with a unique power spectrum, so the problem becomes one of categorizing the different kinds of spectra. The procedure adopted has been to use the perfect infrared source as the standard. It can be shown that a perfect radiator is a perfect absorber, and since absorbers of visible radiation are black, the name adopted for the perfect source is the *black body*.

The radiation emitted from a black body has a power spectrum which is dependent only on the temperature of the black body. Figure 60 shows a typical radiation curve for a black body at 1500°C. The values of this curve are given by Planck's Law:

$$W_\lambda = \frac{37415}{\lambda^5}\,\frac{1}{e^{-14388/\lambda T}{}_{-1}} \qquad (17)$$

where

W_λ = spectral radiant emittance, $W/cm^{-2}\mu^{-1}$

λ = wavelength in microns, μ

T = absolute temperature, °K

and we have expressed the constants as numbers rather than giving them as combinations of more fundamental constants.

[11] The image converter changes an image formed at infrared wavelengths into one at optical wavelengths, thus making it visible to the human eye.

[12] Most of this historical information is derived from Richard Hudson, Jr., *Infrared System Engineering* (New York: John Wiley and Sons, 1969), pp 3-9.

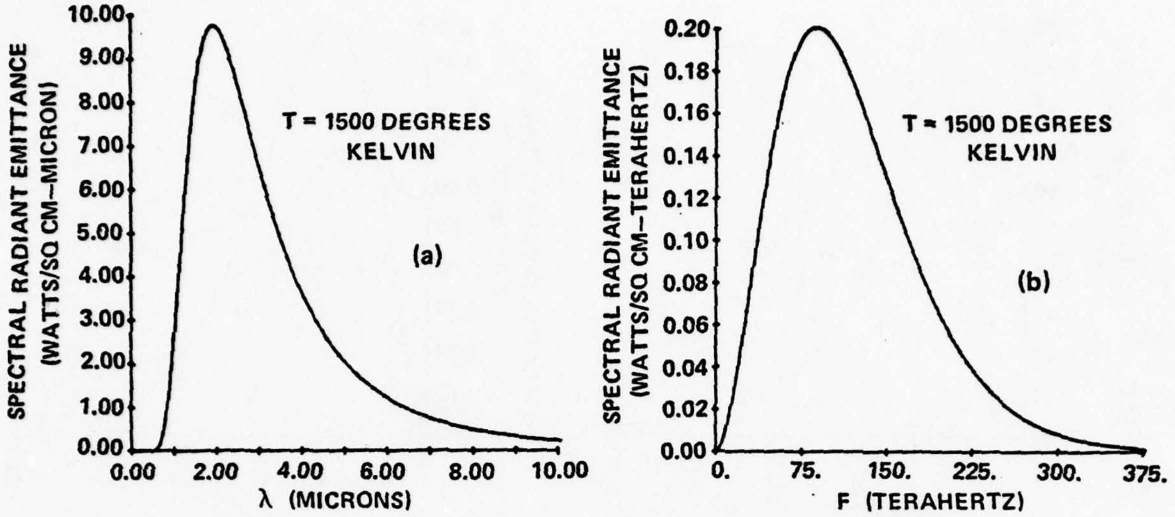


FIGURE 60. TYPICAL BLACKBODY CURVES

We ought to note that the spectral radiant emittance is basically watts per unit wavelength per unit surface area, rather than the watts per hertz common to electromagnetic warfare. This is first a reflection of the fact that we are dealing with natural objects as radiators instead of a fabricated generator, thus the source has a physical size, and the bigger the object the more energy radiated. Secondly, at this high frequency, measurements have traditionally been made in terms of wavelength rather than frequency because wavelength can be directly measured with a simple instrument, a ruler, while the frequency must be a derived value.[13] To permit a comparison of infrared emission with more familiar terms, Figure 60a has been redrawn (Figure 60b) as a power spectral emittance in watts per square centimeter per hertz.[14] We might also note that the unit of wavelength traditionally used is the *micron* (10^{-6} m) which also is called the micrometer using the standardized prefixes being advocated for the electrical engineering profession. The unit of temperature, degrees Kelvin, is related to temperature in degrees Centigrade by the following expression:

$$°K = °C + 273 \qquad (18)$$

Since the infrared power spectrum varies with temperature we need to inquire what this variation is. It is given by Wein's displacement law:

$$\lambda_m T = 2898 \qquad (19)$$

which relates the wavelength of the maximum of the curve, λ_m, to the blackbody temperature. This convenient relationship allows one to draw universal blackbody curves in terms of λT or f/T and the percent of maximum emmission (Figure 61). Of more use to us may be the curves drawn on logarithmic scales (Figure 62). From these plots it is clear that the bandwidth of the blackbody is 120 percent of the center frequency on a wavelength scale and 150 percent on a frequency scale, which makes the blackbody a broad-band emitter.

[13] This is a reflection of the fact that up to the present much of the work in infrared might be classed as physics, obtaining a fundamental understanding of the physical process which occurs. As infrared becomes more widely used, especially in communications applications, the engineering unit of hertz may be more common.

[14] This curve has a different shape than the wavelength curve because frequency and wavelength are inversely proportional quantities.

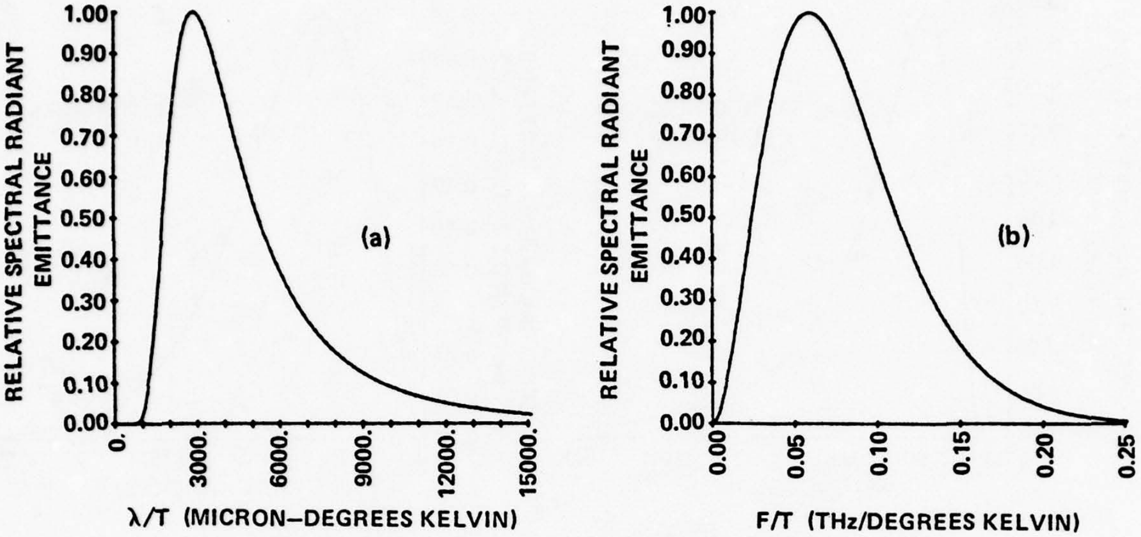


FIGURE 61. UNIVERSAL BLACKBODY CURVES

The blackbody, as the standard radiator, can be achieved in the laboratory to an accuracy of better than one percent over a small surface. But natural objects typically do not radiate as much energy as blackbodies, and three additional terms are used to describe their deficiencies. The *emissivity* ϵ, is the ratio of the spectral radiant emittance at any wavelength to that of a blackbody of the same temperature at that wavelength. If the emissivity is constant over all wavelengths then the object is called a *greybody*. If the emissivity varies as a function of the wavelength, often indicated by writing $\epsilon(\lambda)$, then the object is called a *selective emitter.* For a selective emitter one must construct a table of $\epsilon(\lambda)$ versus λ, or plot a curve, in order to completely describe the object. In all cases, since the blackbody is the perfect emitter, the emissivity is always less than unity.

Because every natural object emits infrared, the radiation from any particular object of interest, usually called a *target*, must be distinguished from surrounding radiators. Thus every object exists in a *background* of radiation, and this background varies as different objects are selected.[15] Hence one of the major problems in applying infrared technology to military uses is to determine how to distinguish the target from the background. This problem can be succinctly stated as "one man's target is another man's background".[16]

Backgrounds are commonly broken into three general classes: sky, earth, and marine. Each of these has their own general characteristics which are summarized in Table 31. As you can see, backgrounds are characterized by both greybody and selective emissions. If a particular infrared design is needed, much more detailed information is available.[17]

Of course the real interest in infrared systems is in the targets. Each particular target has its particular characteristics, of most interest to us are aircraft. The major infrared producing components of an aircraft are the engines, and the structure itself at high

[15] One might eliminate this problem by actively illuminating the target, but before the advent of the laser high-power illuminators were too large and costly for airborne applications.

[16] M. R. Hoter, et. al., *Fundamentals of Infrared Technology* (New York: MacMillan Company, 1962), p 29.

[17] See Hoter, *Fundamentals of Infrared Technology* and W. L. Wolfe, *Handbook of Military Infrared Technology*.

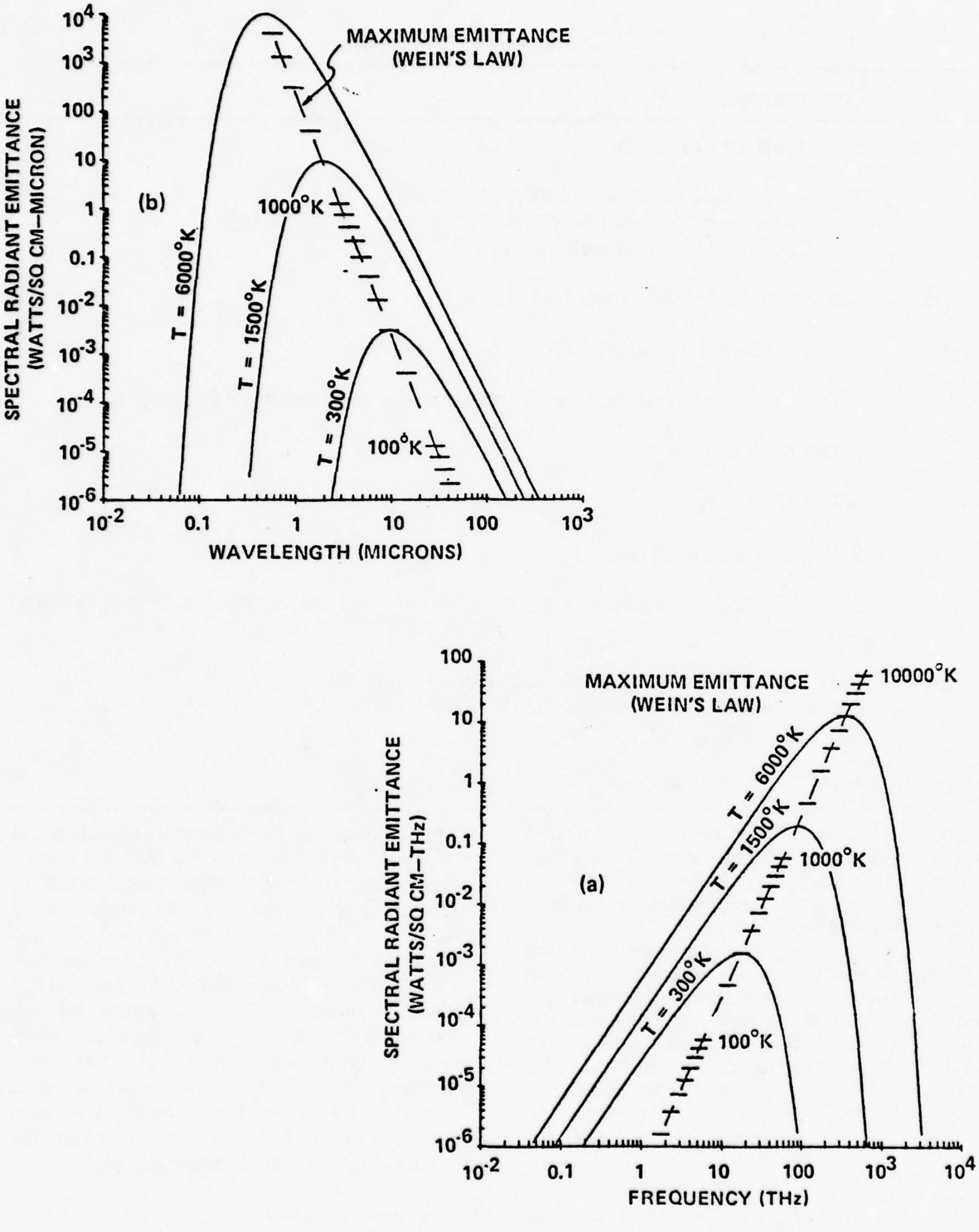


FIGURE 62. BLACKBODY SPECTRAL DISTRIBUTION CURVES

Table 31

Background Characteristics

Type	Components
Sky	Solar Scattering ($\lambda < 3\mu$). Thermal emission ($\lambda < 4\mu$) 300°K blackbody Water vapor emission bands: 0.94, 1.1, 1.4, 1.9, 2.7, 6.3μ Carbon dioxide emission bands: 2.7, 15μ
Aurora	Emission lines at 0.92. 1.04, 1.11, 1.5 – 1.6μ
Airglow	Emission lines at 1.6 and 2.5μ
Stellar	Blackbodies dependent on effective temperature and magnitude (brightness)
Planet	5900° K blackbody
Solar	6000° K blackbody
Clouds	Solar Forward scattering
Earth	300° K greybody modified by terrain emissivity and reflectivity, and atmosphere absorption
Marine	Reflectivity depends on sea surface layer (0.1 mm thick) Emission depends on temperature (0° – 29 °C) Sea water opaque for $\lambda > 3\mu$

NOTE: Data derived from Wolfe, *Handbook of Military Infrared Technology*.

supersonic speeds. It is clear that infrared signature data on military aircraft is tightly controlled, however, there is enough published data that we can determine their important characteristics.

For a turbojet engine the potential sources of infrared energy are the engine itself (that is, the combustion chambers and other hot metal parts), the tailpipe opening and the plume of hot exhaust gasses. But the hot engine parts are invariably shrouded for aerodynamic reasons, so that they are effectively shielded. Thus the major components are the tailpipe opening and the plume.

An analysis of the temperatures, pressures and gas composition inside a turbojet engine shows that for engineering calculations "a turbojet engine can be considered as a greybody with an emissivity of 0.9, a temperature equal to the EGT, and an area equal to the exhaust nozzle."[18] The EGT is typically limited to a maximum of approximately 900°C by turbine-blade temperature limitations, with operating temperatures of 700°C for takeoff and 500-600°C for cruise. The exhaust nozzle area is approximately 3.600 square centimeters for a typical 16,000 pound thrust engine.[19]

[18] Hudson, *Infrared System Engineering*, p 87. EGT is the exhaust gas temperature.

[19] *Ibid.*, p 90. The Pratt and Whitney JT4A-9 engine used on the Boeing 707-320 has a nozzle area of 3,660 square centimeters.

The plume of a turbojet is composed of hot gasses, of which the principle components are carbon dioxide and water vapor. Consequently the maximum emissions occur around 2.8μ and 4.4μ with the later being between two and 10 times more intense, depending upon the exact combustion conditions. The temperature of the plume continuously decreases away from the nozzle with the result that any calculations should use measured data for accuracy. However, a calculation of the gas expansion through the temperature of the plume at the nozzle is about 15 percent lower than the EGT.

about 15 percent lower than the EGT.

The actual radiation from the plume depends upon its temperature, its composition and its size, the exact relationship being:

$$I = 5.6697 \times 10^{-12}\, \epsilon A(T_p^4 - T_r^4) \qquad (20)$$

where:

I = radiant emittance, watts
ϵ = emissivity
A = surface area, cm^2
T_p = plume temperature, °K
T_r = reference temperature, °K

It is clear that plume temperature has a very strong effect on the quantity of energy radiated, but this effect is independent of engine size. However, the fact that the temperature dependence is the difference between the gas temperature and a reference temperature individually raised to the fourth power has an important effect on the directional characteristics of the plume radiation. For as the gasses in the plume recede from the engine they cool and become absorbers of the radiant energy emitted by the portion of the plume nearer the engine. Thus the plume radiation is almost completely absorbed directly to the rear of the engine.

Equation (20) also shows that the radiant energy depends upon the surface area of the plume. Hence larger engines radiate more energy. Likewise, higher engine power settings create more radiation both because the engine temperature increases, thus increasing plume temperatures, and because the increased fuel consumption produces a larger plume. The third factor, emissivity, is both a function of frequency or wavelength (thus yielding the double-peaked spectral distribution mentioned earlier) and also a function of the physical conditions of the gas. This yields another important effect relative to engine size. Any text in heat transfer[20] has data showing that the emissivity of gas molecules depends on the gas pressure (partial pressure in this case), the gas temperature and the diameter of the emitting region. The gas partial pressure depends upon combustion conditions but not on engine size if the engine designs are similar; but the diameter of the plume and its apparent temperature do vary with engine size. The published data shows that emissivity can vary between the one-half and first power of the plume diameter with the temperature moderating this relationship slightly. But temperature variations influence the total radiation as the fourth power. The result of these complex interactions is that it is not unusual to have the plume emittance of a series of engines increase as the 3.5 power of the engine diameter.

Since the plume radiation depends upon the fuel consumption it typically decreases by a factor of two between sea level and 35,000 feet. Carrying out the necessary calculations shows that the radiant intensity of the plume averages about 10 percent of that of the nozzle for non-afterburning, subsonic flight so that the plume is often neglected in calculations.[21]

There are two engine modifications which change these figures. One is the addition of a

[20] For example, Robert Siegel and John R. Howell, *Thermal Radiation Heat Transfer Vol III, Radiation Transfer with Absorbing, Emitting, and Scattering Media,* NASA SP-164 (Washington, DC: National Aeronautics and Space Administration, 1971), pp 24-32; and John H. Perry, *Chemical Engineer's Handbook* (New York: McGraw-Hill Book Company, 1963). Chapter 10, pp 40-43. Siegel and Howell may be obtained from the Superintendent of Documents, US Government Printing Office, Washington, DC 20402.

[21] Hudson, *Infrared System Engineering,* p 95.

fan driven by the turbine–the turbofan engine. The turbofan engine with a forward fan surrounds the plume with a cold sheath of air so that the plume becomes much smaller. If the fan is mounted aft, behind the turbine, then cold air is mixed with the exhaust gasses so that both tailpipe and plume temperatures are reduced. Thus the turbofan engine with aft fan could significantly reduce the infrared engine signature.

The other modification, the afterburner, has the opposite effect. An afterburner uses the excess oxygen in the exhaust gasses (provided to keep EGTs within the turbine limits) for the combustion of additional fuel injected into the tailpipe. The temperature of this combustion is limited only the temperature limits of the tailpipe walls, thus temperatures of 2000°C can be maintained. As a result the tailpipe and the plume become much hotter. For the JT4A series engine, the plume radiance can increase as much as 50 times due to both the temperature increase and the (typically) five-fold increase in fuel consumption. Under these conditions, the radiant emission from the plume can become greater than that from the tailpipe.[22]

One of the major reasons for modifying engines with afterburners is to obtain the thrust necessary for supersonic speeds. However, the supersonic flight regime has different aerodynamic characteristics, so we could expect that the infrared characteristics of an afterburning engine might change with increasing Mach number. In fact it does, and the cause is the increasing ram pressure at the engine inlet which makes the engine less efficient. As a result the nozzle exhaust gas temperature[23] at Mach 3 can fall to approximately one half of its value at subsonic speeds. This results in a five-fold decrease in plume radiance. At Mach 3.5 the plume radiation from high supersonic speed aircraft again becomes a small fraction of the tailpipe radiation. These variations are illustrated in Figure 63.

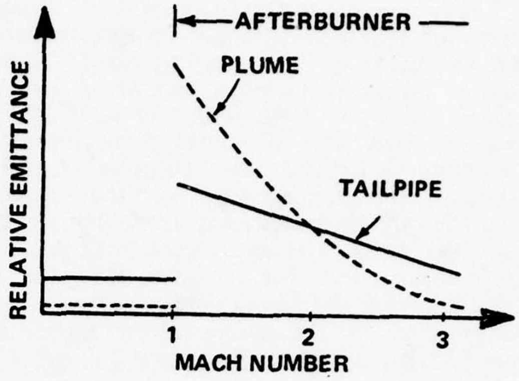


FIGURE 63. TYPICAL TURBOJET ENGINE INFRARED EMISSION

The other major infrared source on an aircraft is its structure at high supersonic speeds. The maximum possible structural temperature is the stagnation temperature of air at the speed of the aircraft. This temperature is given in Figure 64. If the aircraft is flown in sustained supersonic cruise for a long enough time, then the leading edges of the structure will attain the stagnation temperature. But above Mach 2, the stagnation temperature is high enough that structural weakening may occur. Consequently, the temperature rise may be limited by limiting the flying time at high Mach numbers, or by cooling exposed surfaces with fuel.

These high temperatures have two effects of interest to us. First at high Mach numbers the radiance of the structure may become appreciable in the forward hemisphere. Thus suppressing the engine radiation in those flight regimes has only marginal value. Second, the high skin temperatures may seriously interfere with any infrared sensors aboard the aircraft. Thus EW systems for use on high-speed aircraft have to be carefully designed.

Infrared Propagation. Even though we can generate infrared energy, it is useless if we

[22] *Ibid*, p 98.

[23] By this we mean the temperature of the exhaust gasses as they exit the engine, not the EGT; the EGT is measured after the turbine but before the afterburner for the purpose of monitoring turbine temperatures. Consequently EGT does not change with afterburning.

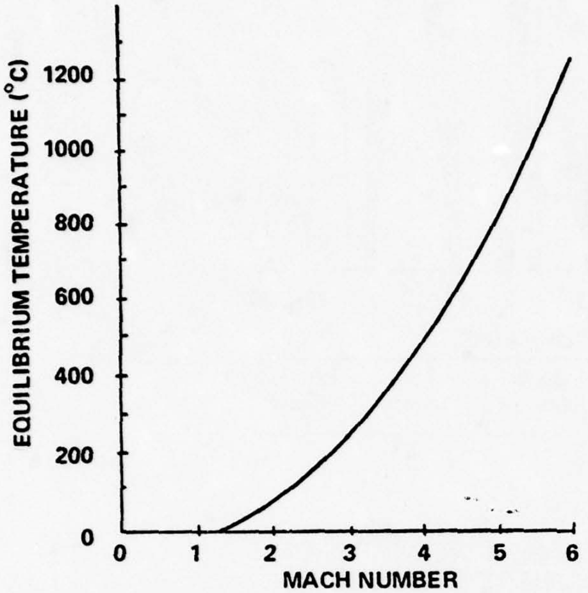


FIGURE 64. STAGNATION TEMPERATURE VERSUS MACH NUMBER (FOR ALTITUDE ABOVE 37,000 FT AND LAMINAR FLOW).

cannot transport it to its destination. In many military applications this means transmitting it through the atmosphere. However, the atmosphere is not equally transparent to all wavelengths. The gas molecules (principally water and carbon dioxide) act to absorb[24] the energy at certain wavelengths, thus creating "windows". There has been a large amount of detailed measurements on atmospheric propagation in the infrared which can be found in the references cited previously. For our purposes Figure 65 will suffice to illustrate the phenomenon. This figure represents a smoothed version of data measured over a 300 meter path.[25] In general, the percent transmission varies very erratically at the longer wavelengths so that only regions of 0 or 100 percent transmission are accurately represented in the figure.

In addition, ozone has an infrared absorption band at 9.6μ. At sea level this band is obscured by the absorption bands of water and carbon dioxide, but in the stratosphere, at an altitude of about 25 kilometers (80,000 ft) where the water vapor and carbon dioxide concentrations are low, there is a significant ozone concentration. Thus this absorption band might be significant to high flying aircraft.

Not only do atmospheric gasses absorb infrared, but particles in the atmosphere scatter the energy also. The amount of scattering depends upon the relative sizes of the particles. Particles much smaller than a wavelength produce very little scattering; those much larger than a wavelength scatter independently of their wavelength; and the scattering changes rapidly with size for particles with radii approximately equal to a wavelength. Thus the scattering of infrared by the atmosphere depends upon the weather phenomena and the wavelength. Table 32 lists typical particle sizes encountered in the atmosphere. From this table it is clear that infrared does give some increased visibility over visual wavelengths (.4 to .8μ) in haze, but in other weather conditions infrared has no advantage. Thus as long as we are constrained to work within the atmosphere, infrared systems can never qualify as all-weather systems.

The final atmospheric effect is scintillation due to variations in the refractive index arising from temperature inhomogeneities. This is a small scale effect in that points separated by more than 5 minutes of arc (1/12 of a degree) scintillate independently. The scintillation frequencies are usually below 100 Hz with deviations up to 9 seconds of arc and intensity modulations of up to 10 percent being observed. Thus scintillation is most likely to be significant in high accuracy tracking systems.

Infrared Detectors. The final component in any infrared system is the detector, the sensor

[24] We should note that since objects that absorb infrared also emit infrared (the so-called Kirchoff's law: "Good absorbers are good emitters"), the function of atmospheric gasses as absorbers or background radiation emitters depends upon the relative temperature of the atmosphere and the source.

[25] Wolfe, *Handbook*, pp 252-254.

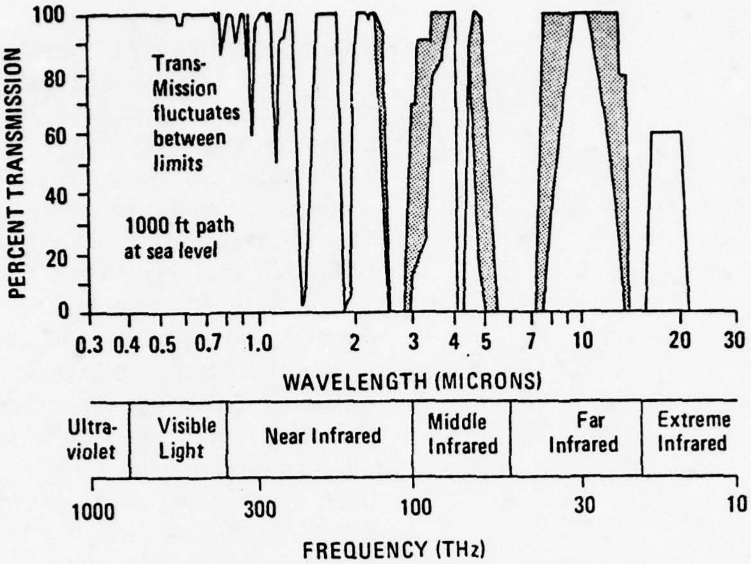


FIGURE 65. TYPICAL INFRARED TRANSMISSION THROUGH THE ATMOSPHERE (ADAPTED FROM HOTER, et. al., pp 410-412)

Table 32

Atmospheric Particle Size

Haze	0 - 0.5μ
Mist Fog Cloud	0.5 - 80μ
Rain	250 - 3000μ

Table 33

Infrared Detectors

Imaging	Point
Infrared Film	Thermal
Image Converter	Photon
Infrared Vidicon	
Evaporograph	
Infrared Sensitive Phosphor	

that converts infrared energy to an electrical signal. Although there are a large number of infrared detectors they fall into two groups listed in Table 33: imaging detectors which yield a picture-like rendition of the target and its background. Obviously, a point detector can be used to build up a picture of the target and its background by scanning, the major limitation is the time required to complete one scan. Conversely an imaging detector may be considered a myriad of point detectors operating in parallel. Both types of detectors have their applications to warfare, but in general the imaging detectors have been used where it was important that a man look at the scene. Of the imaging detectors only the infrared vidicon and the image converter have a sufficiently short image processing time that they can be used for direct viewing of a scene. In addition, if photoemissive surfaces are not used, both these devices can be extended to work to 10–15μ. Finally, the vidicon has a built in storage feature which integrates the incoming energy per image element, thus providing a processing gain. Unfortunately none of the imaging detectors are as well developed as the point detectors.

In military uses where target-tracking or search-radar type operation is desired, the point detectors have been almost universally used, so we will discuss them in more detail. Even here, however, when the scan time becomes excessive, it is customary to employ an array of point detectors to reduce the scan time. This array suggests a miniature imaging detector scanning a large scene.[26]

The point detectors also fall into two classes listed in Table 34, called thermal detectors and photo or quantum detectors. In the thermal detectors the heating effect of the incident radiation causes some electrical characteristic of the detector to change. Since heating is involved these detectors have a relatively long response time, but if they are well made–i.e., they are "black"–then they respond to all the infrared frequencies.

Table 34

Infrared Point Detectors

Type	Time Constant (μsec)	Useful Wavelength (μ)
Thermal		
Thermocouple	25,000	1 - 40
Thermopile	5,000	1 - 40
Bolometer	2,000	0.2 - 40
Low Temperature	5 - 2,000	400
Pneumatic (Golay detector)	20,000	1 - 1,000
Photon		
Photoelectric	1.25 max	
Photoconductive		
Pbs	50 - 5,000	6 max (intrinsic)
Others	0.1 - 150	160 max (doped)
Photovoltiac	0.01 - 300	15 max
Photoelectromagnetic	0.1 - 1	8,000 max

The photon detectors, on the other hand, detect incident photons by means of electrons that are directly displaced by the photons. There are four mechanisms that are used to detect the displaced electron and these give raise to four different type of photon detectors. These four processes are also characterized by different energies required to displace the electron.

a. *Photoelectric.* The electron is knocked out of the material and collected on some other electrode. This requires at least .98 electron volt for materials such as silver oxygen cesium (S-1) surfaces.

b. *Photoconductive.* The displaced election and the site it left, called a hole, act as charge carriers and modify the conductivity (resistance) of the bulk material. The material is typically a semiconductor. If it is pure it is called an intrinsic semiconductor and the energy required to displace an electron (called the band gap) is in excess of 0.18 electron volts at room temperature. However, the characteristics of the material may be modified by doping, the addition of minute quantities[27] of an impurity, in which case the material is called an extrinsic semiconductor. This can reduce the band gap energy to 0.0088 electron volts (Boron-doped germanium, Ge:B).[28]

c. *Photovoltiac.* The electron is displaced in the vicinity of a semiconductor p-n junction. The internal electric field from the junction separates the electron and the hole and the result is a potential difference across the detector. The minimum required energy is 0.083 electron volts in mercury-cadmium-telluride (HgCdTe).

d. *Photoelectromagnetic.* An external magnetic field is used to separate the displaced electron and its hole. This requires an energy of at least 0.177 electron volts in

[26] Dennis C. Lacy, "Infrared Physics and Systems Considerations" (Course notes, Course 367.12, Avionics Systems Engineering, UCLA, July 1972).

[27] How minute is shown by copper-doped germanium where there is one impurity atom for every four million germanium atoms.

[28] The shorthand notation for a doped semiconductor is to write the bulk material first with the dopant following a colon.

intrinsic (pure) semiconductors but doped semiconductors have been made with band gaps as small as 0.00015 electron volts (indium antimonide, InSb).

Since the energy of a photon is directly related to its frequency, the minimum required energies translate into a maximum or cutoff wavelength. Figure 66 shows the relationship between photon energy and wavelength and thus the cutoff wavelength of each type of detector. Clearly, extending the cutoff of a detector type is a search for materials with smaller band gaps.

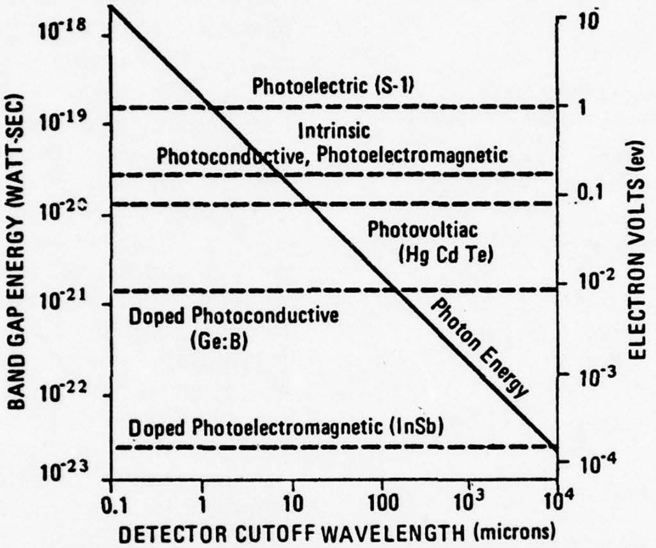


FIGURE 66. BAND GAP ENERGY VERSUS DETECTOR CUTOFF WAVELENGTH

The minimum incident energy a photon detector will respond to, or its sensitivity, is also an important parameter. Sensitivity is a more difficult characteristic to address than cutoff because photon detectors respond to photons, not power or energy *per se*; so their frequency response is flat only when the number of photons per unit frequency is constant, which is not the usual test case. Usually their sensitivity, called detectivity D,[29] is plotted for constant incident energy, so that their response rises until their cutoff frequency is reached, as Figure 67 indicates. (This is in contrast to the thermal detector which has a flat response because it senses energy).

There is a theoretical limit to photon detector sensitivity. In Figure 68, we have plotted both the theoretical limits for photovoltiac and photoconductive detectors and the peak detectivity (at cutoff) of some detectors to show how close we come to the limit.

A limitation on photon detectors is their need for cooling. Generally speaking photon detectors that respond beyond 3μ require

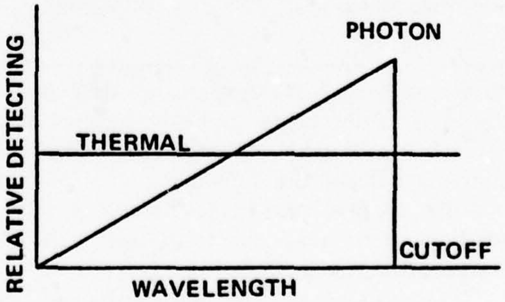


FIGURE 67. THEORETICAL DETECTIVITY CURVES

[29] Detectivity is the reciprocal of the signal (energy) level giving a unity signal-to-noise ratio in a one hertz bandwidth for a one square centimeter detector.

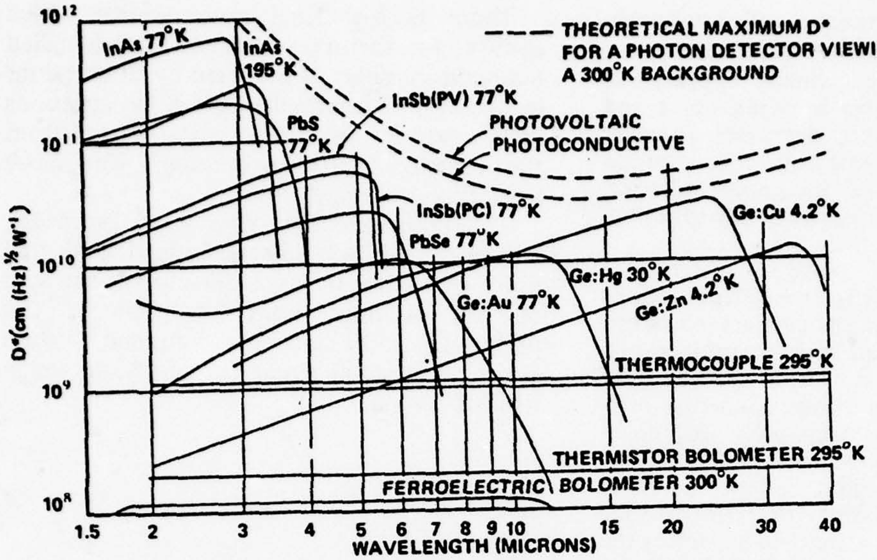


FIGURE 68. THEORETICAL AND EXPERIMENTAL DETECTOR PERFORMANCE (ADAPTED FROM HUDSON, 1969)

cooling. The requirement arises from the need for available charge carriers which can be excited by photons. But the excitation energies available from long wavelength photons are so low that all the charge carriers which could be used will be thermally excited *if the detector is not cooled.*[30] *Figure 69* indicates the general cooling requirement by plotting the detector temperature versus its cutoff wavelength. Also indicated on the chart is a line where the noise power per unit bandwidth (thermal temperature) equals the photon energy (photon temperature), which in general would be expected to bound the detector performance.

The final topic concerning detectors is noise. Noise is not a factor in active electronic warfare because jamming and deception signals must be greater than the signal to be effective. But noise does limit the maximum performance of a passive sensor, and in an area like infrared, where atmospheric propagation is a definite factor, an understanding of noise is necessary to determine what systems are a threat. Furthermore, if we use infrared systems as warning or search systems, operating too close to the noise level will produce excessive false alarms.

There are in general four types of noise which affect infrared systems. The first is *Johnson* or *thermal* noise due to the random thermally excited motion of electrons. This noise, which is also prevalent in all lower microwave bands, begins to decrease *at infrared* frequencies because of the quantum nature of the electronic process which generates it. This noise is generated by all components of the system but it is most critical in components associated with the sensor since later amplification cannot increase the resultant signal-to-noise ration. Fortunately, cooling the sensor will decrease thermal noise. Another potential approach is to amplify the incoming signal using a laser.

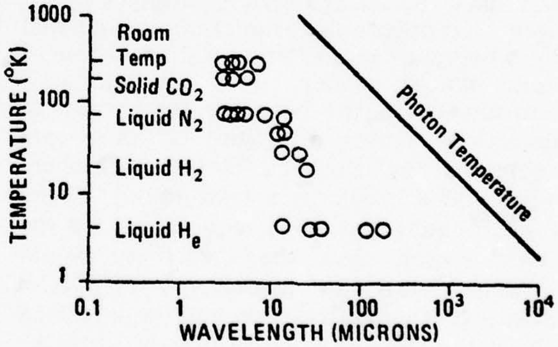


FIGURE 69. DETECTOR CUTOFFS VERSUS TEMPERATURE (ADAPTED FROM HUDSON, 1969 AND WOLFE, 1965)

[30] Or, using the idea of photon temperature developed in the section on optical wavelengths, we could say that the photon temperatures become less than the device temperatures, so that the detector responds to its surroundings.

The second type of noise is called variously *1/f, modulation* or *excess* noise. It is a very low low frequency noise which appears at frequencies below a few hundred hertz and increases as the frequency decreases. In order to eliminate this source of noise it is common practice to "chop" the incoming radiation with a mechanical shutter (a rapidly spinning, vaned wheel).

The third type of noise is *generation-recombination* noise. It is due to fluctuations in the rate at which charge carriers (electrons and holes) are generated and recombined in a semiconductor. Thus it is the equivalent of shot noise in vacuum tubes. Generation-recombination noise is principally found in photoconductors where the generation-recombination phenomenon is the basis of detection and is absent in photovoltiac detectors where the electric field separates the charge carriers. It is for this reason that the photovoltiac curve in Figure 68 is greater than the photoconductive curve.

The fourth type of noise is *radiation* or *photon* noise and is the type of noise discussed previously under optical wavelengths. Infrared is the region in which this noise becomes predominant, thus the shorter wavelength detectors are affected more than long wavelength detectors.

Photon noise affects detectors most through noise associated with background radiation. If the background radiation were constant and noise free, it could be neglected; but since the background radiation is noisy, even if all other noise sources were eliminated by chopping and filtering the background noise would remain. This limitation on performance is the basis for the maximum detectivity curves of Figure 68 which are computed for detection in the atmosphere with 300°K earth as a background. If the background radiation is reduced, as for the space sensor, then the detectivity would increase. However, laboratory tests have shown that detectivity can only be increased about three orders of magnitude by reducing background temperature. Thus there may be other, hitherto unsuspected, sources of noise which will come to light as technology advances.

There is one final noise source which applies to thermal detectors only, called *temperature* noise. It is caused by fluctuations in detector temperature caused by variations in the rate in which heat is transferred from the detector to its surroundings. This noise has a flat power spectrum.

To summarize this discussion on noise, Figure 70 shows schematically the overall noise characteristic of a detector as the sum of the different noise components. The particular amplitudes and frequency values are, of course, different for each detector in its background.

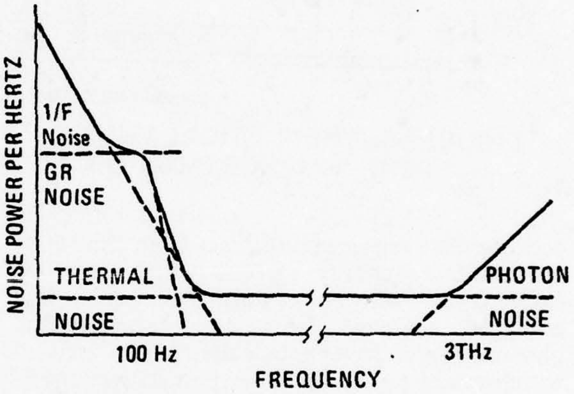


FIGURE 70. DETECTOR NOISE CHARACTERISTICS

Operational Employment. Until recently the tactics and technology of warfare associated with the infrared spectrum have been based upon passive detection systems. SIDEWINDER and REDEYE type missiles have proven to be extremely effective weapons which provide little warning time to their victim. Although the major portion of the remainder of this section will be devoted to the inter-play of tactics and technology with passive detection systems, the advent of reliable and relatively inexpensive lasers will dramatically affect military operations in the infrared spectrum. Laser communication offers the opportunity for very secure, extremely wide band mode of operations.[31]

[31] James Vollmer, "Applied Lasers", *IEEEE Spectrum,* 4.June 1967): pp 66-70 and Bemard Cooper, "Optical Communication", *IEEE Spectrum,* 3 July 1966): pp 83-88.

In addition, laser weapons and their related countermeasures appear feasible in the relatively near future.[32]

In tactical air operations laser rangers have already been tested successfully as well as laser-guided bombs and other munitions. In view of the fact that at this time much of the material associated with military ECM applications is classified and can be expected to remain so for some time,[33] let us turn our attention to the classical use of the infrared spectrum by the military.

The development of infrared systems has been paralleled by the search for effective infrared countermeasures. Possible infrared countermeasures fall into two categories, *design* and *tactics*. Design countermeasures affect the inherent radiation patterns of infrared targets. Tactical countermeasures, which include defensive movement of the target and the use of infrared screens or decoys, complicate the already difficult problem of target discrimination.

DESIGN. The detectability of a target may be considerably decreased by one of several modifications in its design. These include a reduction in the intensity of radiation at its source, shielding of the radiation, or the introduction of counteragents at the radiating source.

1. Reducing the Radiation Level–The most direct means of reducing the intensity of target radiation is by operation of the primary infrared sources at lower temperatures. For subsonic aircraft the primary infrared sources are the engines with large emissions to the rear; for supersonic aircraft the airframe may also become a significant isotropic infrared source due to airframe heating. But even in this case the engines will still be the major source in the rear aspect and the afterburners required for supersonic flight will greatly increase IR emissions in all aspects. Operating engines at lower temperature is usually not desirable from the standpoint of operating efficiency. Reducing tactical aircraft speed also has many tactical implications which may not be beneficial when added up. Directly reducing the radiation level is possible by not operating afterburners, but again the tactical implications may make this undesirable as an IR countermeasure.

2. Shielding the Radiation–A more feasible approach involves the interposition of a shield between the radiation source and possible detectors. This can be done directly on some ground equipment by placing the exhaust pipe and muffler of a vehicle on the underside, or indirectly by erecting a mound of soil or sandbags around an artillery emplacement. On a turbojet aircraft shielding may require shrouding the aircraft exhausts or using a turbofan engine. Or one might consider increasing the size of the condensation trail of the aircraft, since this attenuates the infrared radiation of the tailpipe as much as 50 percent (at the expense of visual detectability). Unfortunately, when an afterburner is used the major portion of the infrared radiation comes from the plume behind the aircraft and this is very difficult to shield.

The problem of shielding is different for a turboprop since the major power takeoff is from the turbine and not from the reaction to the flow of gases. For example, one might be able to divert the exhaust gases around some kind of afterbody and shield the direct radiation from the turbine. Furthermore the strong dependance of radiation intensity on the size of the plume makes any effort to break the exhaust up into several smaller exhausts have potentially high payoff in greatly reduced plume radiation. Hence designing effective shielding requires a good analysis of the target characteristics and its mission.

The effectiveness of shielding a target is also related to the type of detecting equipment being used against it. The narrow spectral range of the photodetector makes it very sensitive to small areas of an active target. When used to detect a vehicle, for example, a photodetector sees only the

[32] Gerry, "Gas Dynamic Lasers", pp 51-58.

[33] Note that it has taken about 20 years for the ECM techniques developed in World War II to become generally available in the unclassified literature.

exposed exhaust pipes, mufflers, radiators and exhaust gases. The radiation from these parts of a vehicle is often highly directional and the signals rapidly diminish when the engine stops.

3. Counteragents–A counteragent is some foreign material added to an IR source to reduce its IR radiation. For example, water or aluminum dust added to a jet engine might not only reduce exhaust temperatures for the same thrust but the increased condensation trail would also provide shielding. (Conversely, afterburners increase IR radiation in part because the incompletely burned fuel adds hot carbon particles to the plume.)

TACTICS. The most effective infrared countermeasures are often tactics. In fact, in the case of jet aircraft which use afterburners tactics may constitute the only effective countermeasures. Generally such tactical countermeasures for aircraft are one of the following six types:

1. Maneuvering the plane out of the range or field of view of the detector.

2. Flying the plane between the detector and the sun to hinder discrimination of the aircraft from its background and possibly blinding the detector.

3. Emitting smoke from the engine exhaust. Although the smoke may make the aircraft more difficult to detect using IR radiation it does make the aircraft easier to see in clear air.

4. Ejecting an infrared flare, a very hot pyrotechnic device which attempts to capture or force a false lock-on of the infrared detector.

5. Using an IR decoy. A decoy is an IR source which looks like an aircraft and which may either be ejected from the aircraft to free-fall or be towed behind the aircraft.

6. Interposing clouds or a fog bank between the plane and the detector by selecting an appropriate flight path. The water vapor in the detection path will either partly or completely scatter the infrared radiation from the plane.

All of the above techniques presuppose awareness by the aircraft crew of the presence and direction of imminent attack, either by interceptor aircraft and/or by infrared-guided missiles. Since intitial engagement by ground-based search and track systems will probably be radar controlled, and since the fire control system of the interceptor aircraft may also be radar-controlled, the initial problem of evading an IR attack often involves the use of radar warning systems. Infrared countermeasures then are concerned chiefly with the evasion of air-to-air (or surface-to-air) missiles which utilize infrared homing devices. Consequently IR countermeasures are only one part of an aircraft's defensive ECM system.

However, if the threat is visual (day) fighters with IR missiles then the radar warning may be ineffective. In this case IR detection and warning devices might be a much better IR ECM aid, if their false alarm rate can be kept low enough (due to the 300°K earth background).

Unintentional Radiation

Heretofore, we have assumed that the signals emanated by us or by the enemy were intentionally radiated; thus their use in electronic warfare becomes one of foiling the purpose for which the signal is used. But are all the radiated electromagnetic signals intented? The answer is clearly "no", for passive IR homing uses an unintentionally radiated signal. The primary source of such radiation is hot objects and the radiation is a by-product of the required high temperatures. In the radio frequency bands the exploitation of such radiation is given one of two names depending on its use. Radiation Intelligence or RINT is the name applied to all efforts to derive intelligence from such unintentional radiation. This differs from SIGINT in that the latter seeks the information contained in intentionally radiated signals, while RINT seeks to exploit signals that the enemy may be unaware he is radiating. Unintentional Radiation Exploitation (URE) is used for all efforts to use such radiation for operational purposes. In both bases, the radiation is non-information bearing, that is, it is not intentionally used for system operation.

An example may make the concept clearer. All of us have heard in an AM or FM radio, the noise from a car with unsuppressed ignition. We consider this noise a nuisance since only a defective ignition produces it. But from a military viewpoint that noise is characteristic of a gasoline engine. Thus reception of that noise indicates that a gasoline engine is in the vicinity. The circumstances would indicate whether it were a car or a truck, or some other equipment.

The ability to identify gasoline engines, for example, becomes more significant when it is realized that tactical electronic equipment must of necessity be self-contained. Thus a tactical radar will have some sort of electrical generating equipment nearby. Even if the radar is shut down–emission control–unless its engine-driven generator is shut off its position may be determined from its engine generator. And if weapons are directed against the generator the radar system can be put out of action as effectively as if the radar itself were destroyed.

A second example concerns the radar itself. Most radars require a high voltage pulse to turn the transmitter on and off. This high voltage pulse is similar to the pulse used to fire a spark plug, so it also can cause radiation. Hence even though a radar is radiating into a "dummy load" and not into the atmosphere, it may be detected.

The result is that RINT offers the opportunity to determine enemy order of battle information without enemy knowledge of that fact. And from URE one might develop a *passive homing device* which could use the unintentional signal. Thus we could gain both valuable intelligence and an operational advantage from a knowledge of such unintentional radiation.

Of course, the exploitation of unintentional radiation is not without problems. The primary problem is that the existence of the unintentional radiation must first be discovered before it can be exploited. This discovery is just as difficult as any other ELINT task. The converse is also true, that to avoid similar exploitation we must seek to eliminate all such unintentional radiation. Unfortunately the testing and additional design effort necessary to eliminate unintentional radiation may add significantly to equipment cost. Thus the advantage conveyed to an enemy must be balanced against its cost.

"Smart" Weapons

The final direction which the use of *electronics in warfare* is taking is that of the so called "smart" or terminally guided weapons. Now terminally guided missiles are not new, for active and passive guidance has been proposed and used for air-to-air and surface-to-air missiles for over a decade. What is new is the application of these concepts to air-to-ground delivery of conventional munitions. In the process of developing these terminally guided weapons it has become clear that when the electronics guarantees the delivery accuracy then the delivery aircraft becomes only a weapons transporter. Thus this concept also includes the idea of remotely piloted vehicles (RPVs) as the weapons carrier. Since both terminal-guided, air-delivered munitions and RPVs depend upon radiated electromagnetic signals for their effectiveness we will discuss both. For *the whole objective* of these developments is to replace man as the direct operator of military weapons in order to gain an advantage.

Let us look at terminal-guided weapons first. This term has been applied to such air-delivered munitions such as the laser-guided bomb.[34] The rationale for these weapons is that the destructive effects of conventional munitions against many tactical targets may be determined more by delivery accuracy than any other factor. Trying to design an aircraft bomb delivery system for accurate, medium-altitude delivery suffers from several built-in handicaps. First there is the ballistic dispersion of the bomb itself. Then there are atmospheric factors such as wind. Finally there is the necessity for accurate aircraft control so that the bomb is released from the precise point with the precise velocity required to hit the target.[35]

[34] Richard T. Davis, "Smart Bombs Perform Interdiction Surgery", *Microwaves* (October 1972): p 35.

[35] This translates operationally into the requirement of releasing the bomb at the correct airspeed, altitude, and attitude (bank and dive angle). With conventional, fixed (iron) sights this requires a high degree of skill.

Since the first two factors are beyond our control we have tended to spend all our effort on the last, spending more and more money on sophisticated electronics to assure more accurate delivery. Unfortunately, small inaccuracies are multiplied by the free-fall trajectory of the bombs so that increasing bombing accuracy in this manner leads to skyrocketing costs. Furthermore, the pressures of combat upon the pilot tend to negate much of the design since it is the pilot who must point the aircraft at the target. And as Appendix C shows, the effect of these inaccuracies is magnified many times because we must put our expensive aircraft at risk again and again to achieve our objective, destroy a target.

The "smart" weapon substitutes terminal guidance for the sophisticated aircraft electronics. Terminal guidance has the desirable characteristic that absolute accuracy increases as the target is approached. Hence, terminal guidance offers a clear alternative in weapon delivery. However, we must provide some sort of signal to guide the weapon. Since many targets do not radiate signals, and even if they do the enemy may turn off such signals to escape destruction, it is clear that we must designate the target. The laser with its capability of high-brightness illumination from a distance has provided a low-cost and easily used target designator; a more sophisticated system might use an electronic navigation system.

If one examines the curves in Appendix C, it is easy to show that one can spend a sizable amount of money on an expendable terminal guidance system and still drastically reduce the cost of destroying a target. The major factor in this analysis is not the weapon cost but the attrition cost of expensive aircraft. That being so, then even sophisticated electronic terminal guidance systems may be cost effective, especially for fixed targets.

It is clear that many important targets: supply dumps, choke points on lines of communication, airfields, etc. are fixed—they will not move from day to day. Hence if they are located once, then we should be able to attack them without having to locate them again. But today, even with our present "smart" bombs, we require a pilot in a high pressure combat situation to locate the target a second time. Given this situation, simple camouflage and decoys are very effective; if we could translate the intensive analysis which initially designated the target into unequivocal weapon terminal guidance, the resulting effectiveness might support a considerable system cost in comparison with our present methods. This is not to say that present tactical systems will disappear, for moving targets still require the presence of manned aircraft for rapid strike capability.

A moment's thought will show that air-to-ground weapons delivery is not the only area where human capabilities limit weapons. If the man were removed from tactical aircraft, the necessity to provide a human environment (pressure, temperature, G-limits) could be removed, and the airframe could be designed to limits dictated only by the installed equipment, with possibly an increase in performance. Of course, control equipment must be included to allow tactical mission performance but if we do not require one 2
weapon system to do every conceivable task (as we tend to do with a man) then this equipment could be simplified. Thus the remotely-piloted vehicle becomes a potential contribution to combat effectiveness.

There are several examples or potential examples of RPVs in military applications. If we look at air defense, the BOMARC missile is essentially a RPV interceptor. (We should note that it is always under GCI control, it has a well-defined task.) Then there is the military reconnaissance task. Since the targets are predetermined the task is well defined and a RPV can do the job as well as a manned vehicle. In fact spy satellites could be considered as one form of RPV. In weapon delivery using terminally-guided weapons, the weapon deliverer could be an RPV, since it need only get the weapon in the vicinity of the target. Finally the Soviet Lunokhod is an illustration of the complexity of the tasks and distances over which an RPV can function.

On the other hand, RPVs have a specific vulnerability, and this is where electronic warfare interfaces. Since RPVs must be controlled over enemy territory, there must be some communications link with them. If only a minimal amount of control is needed then the RPV can be preprogrammed to fly the desired course. Now the RPV becomes a drone and one must be prepared to accept navigation errors of up to several nautical miles. If such inaccuracies are unacceptable then direct control must be exercised over the vehicle. This implies a two-way channel since the RPV must not only be flown, but it must report back its postion. With sophisticated design this channel can be protected from ECM and intrusion but such protection probably will not be cheap, especially since the RPV will be power limited and over enemy controlled territory.

RPVs, and "smart" weapons in general, present a challenge in electronic warfare. If they can be made effective and their costs controlled then they are a definite combat advantage to us and a definite threat if used by the enemy. It seems clear, however, that one of their more vulnerable areas may be the communications or guidance signals which must be transmitted. Our electronic warfare efforts must keep abreast of these developments to avoid being surprised by our own vulnerability, as well as to be prepared for any enemy exploitation of these areas.

THE ELECTROMAGNETIC CONFLICT IN SPACE

The previous chapters have generally concentrated on electronic warfare as it applies to air battles involving manned, air-breathing vehicles. What new principles do we have to consider as we move outside the atmosphere into space? If we consider only manned vehicles we eliminate ballistic missile reentry vehicles from consideration. In terms of the current debates on SALT talks, MIRV and the like, such an exclusion seems to be a big loss, but this is only because we are in a period of transition.

To obtain a true perspective let us consider what the situation would be if we had manned space stations in orbit. Then we could make the comparison that as airplanes are to artillery, so space stations are to ballistic missiles. No one in his right mind proposes that we counter artillery by shooting down the shells in flight; instead we attack the guns themselves. Likewise, it would be best to attack the missiles while they are still in their silos or while they are in their boost phase. (The success of the Israeli's in 1967 was due in part to the fact that they destroyed the Egyptian Air Force on the ground.) Hence the real problem of the future will be to protect our manned space stations that perform surveillance and command and control functions.

The Space Environment

To be most effective, a manned space station will have a nearly circular orbit at low altitude (200 to 300 miles).[1] High altitude missions, above 1,000 miles, would have a certain advantage in being hard to detect and destroy because present detection equipment is limited in its range capabilities,[2] but we cannot expect this limitation to last forever. The disadvantages of high altitude orbits are; First, a manned space station would have to have extensive shielding for the crew, because of the Van Allen Belt radiation above 1,000 miles. Second, delays of 2 to 5 days could be incurred in moving to a lower orbit to carry out certain missions. Third, the large quantities of fuel needed for orbit exchanges would reduce the payload available for the primary mission. Lastly, resupply would be more complicated and more costly. These advantages will tend to keep space stations in orbits under 1000 miles for some time.

Potential Space Missions. Let us examine four missions we could reasonably expect a manned space station to perform.

[1] "A Study of Interception Tactics in Space", *North American Aviation, Engineering Department Report # NA 60-66S*, (1960), p 61.

[2] *Space Planners Guide*, (Andrews Air Force Base, Maryland: US Air Force Systems Command, 1965), Chap 1, p 4.

[4] *Ibid.*

The Threat to Manned Space Stations. Given that we have manned space stations performing the above missions, any enemy will consider them as much of a threat as he currently considers airplanes. Furthermore, at their low altitudes they are easily within radar and infrared detection and tracking range. Hence we must be prepared to protect them against enemy weapons.

To destroy a space station, an enemy must be able to detect the presence of the space station, predict its position, and intercept it with a weapon.[8] The obvious means of countering radar and infrared is with electronic countermeasures. This presents the problem of which electronic countermeasures can insure the survivability of a space station. and also be suitable for use in a space station.

Whether ECM can protect the space station depends upon the vulnerability of the station to the defense weapons. The basic elements of vulnerability are the three mentioned above—the detectability of the station, the predictability of its future position, and the ability of the interceptor to reach it—as well as its sensitivity to the weapon's effects. A space station is vulnerable only if it is susceptible to all four of these elements.[9] Since these elements provide the criterion by which we can determine if ECM is effective, we will examine each one in detail.

ECM Criteria. Let us list the criteria that ECM must meet to be effective in protecting the space station.

1. *ECM must insure a high degree of survivability.* That is, ECM must be effective against one or more of the elements of vulnerability to such a degree that the overall vulnerability of the station is very small.
2. *ECM should not interfere with the primary mission* of the space station; on the contrary, it should aid if it is possible.
3. *ECM must be light-weight.* The payload constraints imposed by the costs of space boosters are even more severe than those for aircraft, hence heavy ECM will be severely penalized.
4. *ECM must be small in size.* Again volume will undoubtedly be a premium in a space station in that the boosters will be volume limited.
5. *ECM should have little or no power requirements.* In most of our earth-bound experience primary power requirements are not greatly emphasized because commercial power is so abundant. What we do not see is the large amount of equipment needed to produce that abundance. In space, every watt expended must be produced somewhere in the space station. Consequently, primary power requirements will be equally important

[5] *Ibid.*, p 62.

[6] *Ibid.*, p 63.

[7] *Ibid.*, p 64.

[8] *Space Planner's Guide.*

[9] *Ibid.*

to size and weight in determining the usefulness of ECM.

6. *ECM should not require specialized personnel.* Since space will be at a premium in the station, it will be important to keep the number of different skills required to a minimum. Thus the ECM operators will either have to be trained in other skills or vice versa. In any case, the simpler the ECM equipment the less restrictive the skill requirements.

7. *ECM techniques which do not require resupply are preferable*, since all resupply will probably be by separate booster, or space shuttle.

Space Station Vulnerability

Before we discuss vulnerability let us list the characteristics of the space station we have discussed previously.

1. The space station will be manned.
2. The station will be in orbitsunder 1,000 miles.
3. The station is a threat to the enemy.
4. Manpower will be rotated and supplies will be brought to the space station by another spacecraft or space shuttle.
5. The enemy has an extensive radar and infrared tracking system.
6. A detected station can be identified as friend or foe.
7. The station is maneuverable.

Detectability. Detection is a function of four variables: space station emissivity, reflectivity, physical size, and range.[10] Emissivity of a space station comes largely from the infrared heat radiated from the space stations' outer skin. Infrared detection has high angular resolution, but no range capabilities.[11] The high resolution results in a very narrow field of view so that accurate acquisition information is required. Furthermore, the space station could not detect its use because infrared detection is completely passive—it does not emit energy to perform detection.

Reflectivity is a concern for both optical systems and radar systems.[12] The laser is the most promising visible reflective detector, but today it is not particularly impressive because of its short range due to power limitations.[13] Even if perfected, laser radars would require an accurate acquisition and tracking function, since their beam widths are narrow.

Present radars for space station acquisition and tracking are accurate, but limited in number. The state-of-the-art resolution for satellite tracking radars is roughly 15 feet in range, 1 foot per second in range rate and 0.005 degree in angle measurements above 10 degrees.[14] Our present Spandar F-band radar used by NASA can skin track a 1 square meter target at 600 miles. Again this precision equipment requires extensive and accurate acquisition information. Initial acquisition would probably be accomplished by a system similar to our BMEWS, SPADATS, or over-the-horizon radar.[15] These radars provide preliminary information on the space station's position, range, and velocity. This information is used to position the precision radar mentioned above.

If the effective space station size can be reduced, the signal return to the ground radar station is reduced and the space station will be harder to detect.[16] For instance, if the rounded nose section of a large cylindrical space station can be pointed toward the radar, detection capability by the enemy will be reduced. The size of the space station will be controlled by the mission requirements, but the shape could be made to help reduce detection.

[10] *Ibid.*

[11] If the detector is earth based then accuracy will be limited to about 2 minutes of arc by atmosphere scintillation.

[12] *Space Planner's Guide.*

[13] "Laser Radar for Space Missions—Exploratory Studies of Major Factors" *Report LMSC # A632070* (Sunnyvale, California: Lockheed Missiles and Space Company, 1964).

[14] "More Launches Will Tax Techniques," *Missiles and Rockets, 11* (September 17, 1962): 36-37.

[15] "Spacetrack, Keeping Tabs on What's Out There," *Air Force and Space Digest, 48* (August 1965): 52-53.

[16] *Space Planners Guide.*

The range of a space station will be controlled largely by the mission requirements. However, the less the range from the enemy the easier it will be for him to detect the space station.

Position Predictability. Once the space station has been detected and acquired, prediction of its position is based solely on accurate tracking. Since position predictions is absc'utely essential for interception, accurate tracking is a definite requirement for an enemy weapon system. There are different types of tracking systems, such as radar and infrared, but in all of them, a computer combines the azimuth and elevation angles of the sensor with a range measurement to obtain the position and velocity of the target. With this information, the computer can predict the target's position. The predicted position will be accurate unless the space station changes its orbit.

It is noteworthy that errors are amplified in the track prediction process so that one desires to track as accurately as possible. If highly accurate sensors are used for tracking, then their high cost means one can only afford a few. With a large number of low accuracy and low cost sensors, computer smoothing must be used to reduce the prediction errors.[17] Pulse radars are usually accurate to tens of feet, but the farther downtrack the predicted position is, the greater this error is magnified.

Infrared can be used to correct the angular errors in radar systems, which are usually larger than 1/2 degree. Infrared can measure space station angles so accurately, that errors are attributed only to imperfections in the sensor and in the atmosphere.[18] Infrared detection is normally used with a continuous tracking radar. When data from these highly accurate sensors are forwarded to a track prediction center, the space station's position can be predicted within a few miles on the first pass. If the space station were to maintain the same orbit for several orbits, prediction error could be reduced to a few hundred feet.[19] Tracking systems would normally be located uprange from the interceptor systems, and toward the direction of the expected threat.[20]

Interception by a Weapon System. Interception is a function of weapon accuracy and of the lethal radius of weapon effects. We have seen that position prediction accuracy would be a few miles. Errors in putting an interceptor in an exact orbit would be small in comparison, together these errors would probably be less than 10 miles. We will briefly look at some interception systems and then at weapon effects.

Ballistic intercept with boost guidance only puts an interceptor rocket at a predicted point and time in space.[21] This type of intercept is not considered since very small maneuvers can always be made which would put the space station outside the weapon effects.

A terminally-guided interceptor is launched to a predicted intercept point and as it approaches this point, the interceptor uses its own sensors to acquire and lock-on the space station.[22] The interceptor then applies a corrective maneuver to intercept the space station. Typically the initial lock-on range is 50 miles w'th a tracking capability of twice this range or 100 miles.[23] To get an idea of the time involved, assume that the space station has a velocity of 4 miles per second. In a head-on intercept (the interceptor coming from the opposite direction) the closing velocity will be at least 8 miles per second With a nominal 50 mile lock-on range, the interceptor must acquire and predict the space station's position and then take

[17] *Ibid.*, Chap 2, p 32.

[18] *Ibid.*

[19] *Ibid.*

[20] *Ibid.*, Chap 2, p 30.

[21] *Ibid.*, Chap 2, p 39.

[22] *Ibid.*, Chap 2, p 42.

[23] *Ibid.*, Chap 2, p 56.

corrective action to intercept the station in little more than 6 seconds. If the space station is not met head on, the time increment may be increased.[24] Still, because the space station is a large target, the interception error of this sytem is zero unless some countermeasures are taken.

A command guided interceptor is also launched to a predicted intercept point, but then the interceptor is directed to the target by the ground radar.[25] Interception errors as determined by the ground radar system would be a few miles.

There exists the possibility that interception may be attempted by another manned space vehicle. However, the maneuverability advantages of an interceptor rocket would be lost due to the greater weight of a manned system. Also, only a small amount of fuel would have to be used by the space station while large amounts of fuel would be required for the manned interceptor to outmaneuver and close the gap between them.[26] Each time the interceptor would make a maneuver to close the gap, the space station could maneuver away. Interception would be extremely difficult at best with the limitation probably being the available fuel.

Because the terminal guidance interceptor is the most accurate, we will consider all interceptors to have this capability. To counter this system, we must be able to introduce sufficient errors into it to keep the space station a safe distance away from the weapons effect. This becomes the goal of our ECM.

Sensitivity to Weapon Effects. There are two types of weapons which are very promising in space: pellets and nuclear weapons. The maximum weapon effects would extend to a few miles for pellets, and to tens of miles for nuclear weapons.[27] Since the nuclear weapon has the largest lethal radius, we will consider all interceptors to have this capability. Obviously, the space station must stay outside the lethal radius if it is to survive.

Hardening is the only way to reduce the space station's sensitivity to weapon effects, and this involves changing the vehicle's skin, and, in general, increasing its weight.[28] In turn, increasing the station's weight reduces its maneuvering capabilities, and thus its capability of moving outside of the lethal weapon effects range. Nevertheless, no matter how much a space station is hardened, a close nuclear explosion will destroy it.

Countermeasures

Electronic warfare capabilities associated with space station survivability consist primarily of threat warning and ECM. Each of these capabilities directly affects the enemy's ability to intercept and destroy a space station. Threat warning is used to detect an enemy radar and tell where the radar is located. ECM is composed of both on-board jamming and expendable jammers. The expendable jammers would be launched in the immediate area around the space station to present many target strobes to the enemy. Other ECM techniques include chaff, flares, and a radar absorbing shield, these either act as a decoy to draw the enemy radar away

[24] *Ibid.*, Chap 2, p 42.

[25] Although the interceptor has more time to make any corrections in non-head-on attacks (due to the lower closing speed), the increased time generally means increased range with its consequent increase in fuel and sometimes a more complicated vectoring problem to achieve intercept. If the interceptor approaches from the rear hemisphere the increased range could exceed the ground radar range, thus degrading mid-course guidance and requiring a greater interceptor terminal guidance capability. Finally, beam attacks require the maximum intercept sensor look angles relative to the interceptor axis. For these reasons it is assumed that head-on attacks will be the most likely.

[26] *Space Planner's Guide*, Chap 2, p 56. Note that if the interceptor has perfect instantaneous information as to the station maneuvers, then his fuel costs would be of the same order of magnitude as the stations. But the inevitable time delays and imperfect information will lead to the situation described.

[27] *Ibid.*, Chap 4, p 3.

[28] *Ibid.*

from the space station or they hide the space station from the enemy. Each category of countermeasures will be compared to each element of vulnerability.

Against Detection. The major technique used to increase survivability during the detection phase is that of warning the station any time a radar is tracking the station. The warning equipment will tell if the radar is friend or foe and where the threat is coming from. Most important, it alerts the crew to a possible attack. Countermeasures would not be used at this time since there would normally not be an attack on the space station during this phase.

Against Position Predictability. Once it is determined that an attack is imminent, a combination of maneuvers and countermeasures, especially decoys, would be highly effective. After detection, the space station could expect to be tracked by other radars so that its position could be refined. Reception of these signals would be a further clue as to an impending attack. Within minutes, position, range, and velocity information would be available to the enemy. It is likely that an attack would be initiated at this time even though the position accuracy would be of the order of a few miles.

When the space station has information that an attack is imminent or that an interceptor rocket has been launched, it could initiate a maneuver, launch decoys in the form of chaff, flares, and expendable jammers, or turn so that a radar absorbing shield on the tail would face the ground radar systems. This would force the ground radar systems to try to determine where the space station actually is, recompute its predicted position, and make a correction to the intercept point.

In maneuvering, a 2 degree change in azimuth alone would move the space station over 42 miles from the point of interception in 5 minutes. With a 3 degree change, the space station would be over 60 miles away from its predicted interception point. This would put the space station outside of the interceptor's nominal lock-on range. Chaff decoys, giving the same reflected radar image as the space station, could be launched simultaneously with an infrared flare to present multiple targets to the ground and interceptor radars. One of the chief limitations of chaff and flares in the atmosphere is their lack of movement. In space this would not be a problem since any object set in motion in space remains in motion. A chaff system which could operate in space has already been developed.[29]

Radar absorbing material can greatly reduce the radar reflectivity of the space station. When used with decoys, the space station may be hidden so well that the ground radar may completely lose the station. Obviously, this would be a tremendous advantage. These radar absorbing materials are not ideal for other functional surface requirements, so they would not be suitable for the primary station skin.[30] Thus these materials must be added and their weight penalty accepted.

Electronic jamming by the space station alone against ground radar may not be advisable because two radars could use the jamming as a beacon and through triangulation determine the position of the space station. However, if used with expendable jammers launched from the space station, multiple jamming strobes would show on the tracking radar systems, each with a trajectory and velocity of its own. These countermeasures could so complicate the prediction phase that the space station might not even be detected by the interceptor. An attack against .his tactic could not be expected to produce results unless it used several interceptors, and if the space station were lost by ground radar, there would be little chance that the station would be intercepted.

The warning equipment and the radar absorbing shield would contain most of the weight of this defensive system. An expend-

[29] J. H. Henson and J. W. Craig, *The Dispensing and Behavior of Chaff in Space*, ASD TN 61-37 (Wright Patterson AFB, Ohio: USAF Aeronautical Systems Division, 12 April 1961). One simple launch technique is pneumatic, using the internal air pressure of the station.

[30] *Space Planners Guide*, Chap 4, p 2.

able chaff, flare, or jamming decoy, if ejected into an orbit using air pressure, would probably weigh under 2 pounds

Against Interception. The objective of maneuvering an ECM is to be outside of the lethal radius of weapon effects. If the countermeasures have been effective during the interceptor boost and mid-course phase, the interceptor will not be in a position where its terminal guidance will be effective. Once the interceptor locks on with his terminal guidance system, normally between 6 and 10 seconds remain until interception. Once again threat warning will be the key to survivability, because the interceptor's radar will be detected long before normal lock on. For the postulated 50-mile interceptor lock-on range, the space station would probably be able to detect the interceptor radar 250 to 300 miles away. This initial warning of the interceptor would call for an immediate maneuver, and chaff, flare, and jamming decoy launch. If the warning includes the direction of the threat, the space station could also be positioned to point its radar absorbing nose toward the interceptor (at the expense of presenting a better target to ground radars).

Jamming from the space station against the interceptor must be done with caution, since an interceptor with a home-on-jam capability would be directed to the space station.

Table 35

The Characteristics of EW Techniques in Space

	Warning	Jamming	Chaff	Flares	Radar Absorbing Shield
Essential to Survival	x	–	x	x	–
Insure Degree of Survival	x	x	x	x	x
Mission Noninterference	x	x	x	x	x
No Extra Personnel	x	x	x	x	x
Low Power	–	x	x	x	x
Light Weight	–	x	x	x	–
Small Volume	–	x	x	x	–
Resupply	–	x	x	x	–
Aid Primary Mission	–[1]	–	–	–	–

[1] Possibly

However,a home-on-jam interceptor could be decoyed to an expendable jammer away from the space station. Jamming tactics are used to the greatest advantage when there are a large number of separate jamming stations and they mutually help one another causing multiple target strobes. The whole survival tactic is based on the ability of the space station to confuse the enemy long enough to allow it to maneuver out of the range of the lethal effects of the interceptor.

The Usefulness of Countermeasures. We shall now compare the different types of countermeasures against the criteria we listed previously (see Table 35). Threat warning is a mandatory requirement for a space station, since it is the warning system against attack. Its equipment is heavy, uses power, and takes usable space, but it could aid the primary mission.

Chaff is essential to survivability, because as a decoy, it draws the attention of a radar away from the space station. Chaff is very light, small, and easy to use. It makes an excellent decoy in space and requires no power.

Flares have the same characteristics as chaff, and when these two are used together, they could counter all ground detection systems plus the interceptor system. However, they are heavier and dangerous to handle and store.

Expendable jammers could increase survivability when used as a decoy. They would not interfere with the crew mission, and would not require specialized personnel. They are also small, light, and carry their own power source.

A radar absorbing shield is not necessary for survivability. By maneuvering the space station to give a minimum cross sectional view, the radar return to a radar would be reduced. The absorbing shield would help survivability because it would further reduce the radar return to the point where the ground radar may lose the station. This is particularly true when decoys are also being used against the enemy radar. The shield needs no power and takes up no interior room, but it would be heavy.

Finally threat warning equipment and a radar absorbing shield would not have to be resupplied, but chaff, flares, and jamming decoys may have to be resupplied as they were used.

Summary

In the environment required for military space missions, electronic countermeasures can reduce the effects of three of the basic elements of vulnerability. After looking at the capabilities of the different types of electronic countermeasures and comparing these to the list of criteria, we can make a few general statements. First, threat warning seems to be absolutely necessary. Second, chaff, flares, and expendable jammers appear to be most promising because of their light weight, small volume, simplicity of use, and deception capability. Third, a radar absorbing shield, while not being absolutely necessary, can be very effective in hiding the space station. All of these countermeasures used together would insure a high degree of survivability of any space station against attack

However,a home-on-jam interceptor could be decoyed to an expendable jammer away from the space station. Jamming tactics are used to the greatest advantage when there are a large number of separate jamming stations and they mutually help one another causing multiple target strobes. The whole survival tactic is based on the ability of the space station to confuse the enemy long enough to allow it to maneuver out of the range of the lethal effects of the interceptor.

The Usefulness of Countermeasures. We shall now compare the different types of countermeasures against the criteria we listed previously (see Table 35). Threat warning is a mandatory requirement for a space station, since it is the warning system against attack. Its equipment is heavy, uses power, and takes usable space, but it could aid the primary mission.

Chaff is essential to survivability, because as a decoy, it draws the attention of a radar away from the space station. Chaff is very light. small, and easy to use. It makes an excellent decoy in space and requires no power.

Flares have the same characteristics as chaff, and when these two are used together, they could counter all ground detection systems plus the interceptor system. However, they are heavier and dangerous to handle and store.

Expendable jammers could increase survivability when used as a decoy. They would not interfere with the crew mission, and would not require specialized personnel. They are also small, light, and carry their own power source.

A radar absorbing shield is not necessary for survivability. By maneuvering the space station to give a minimum cross sectional view, the radar return to a radar would be reduced. The absorbing shield would help survivability because it would further reduce the radar return to the point where the ground radar may lose the station. This is particularly true when decoys are also being used against the enemy radar. The shield needs no power and takes up no interior room, but it would be heavy.

Finally threat warning equipment and a radar absorbing shield would not have to be resupplied, but chaff, flares, and jamming decoys may have to be resupplied as they were used.

Summary

In the environment required for military space missions, electronic countermeasures can reduce the effects of three of the basic elements of vulnerability. After looking at the capabilities of the different types of electronic countermeasures and comparing these to the list of criteria, we can make a few general statements. First, threat warning seems to be absolutely necessary. Second, chaff, flares, and expendable jammers appear to be most promising because of their light weight, small volume, simplicity of use, and deception capability. Third, a radar absorbing shield, while not being absolutely necessary, can be very effective in hiding the space station. All of these countermeasures used together would insure a high degree of survivability of any space station against attack

FURTHER STUDY ON THE ELECTROMAGNETIC CONFLICT

The previous chapters have laid a foundation of the basic principles of the electromagnetic conflict. To proceed further requires that we either discuss the applications of these principles to specific tactical situations or that we discuss the embodiment of these principles in specific equipment. In either case, such information tends to be tightly controlled by the forces concerned, so that information is not available until 20 to 30 years after the fact. Hence, keeping abreast of the current state-of-defense is next to impossible unless one possesses the specific access required. And even so, the fast pace of technology makes it very difficult to be aware of the many factors which may influence this field.

However, restricted access itself creates problems, since the cross-pollination of ideas so necessary for technological and intellectual progress is greatly hindered. This is especially true since the restriction typically applies to technical and tactical details, not operational and strategic concepts. Thus there is a real need for open media for the interchange of ideas. Fortunately such media exist, and it is the purpose of this chapter to provide a short, annotated bibliography of some of these sources. The perceptive reader will note that many of the footnotes in this book are drawn from this list.

But let the casual reader be forewarned that reading every source herein will not make him an instant expert. Many useful articles will not be labelled "electronic warfare". It will take a vivid and creative imagination, or some inside knowledge, to determine the specific application. However, it should be clear that any information relating to the electronic or electromagnetic state-of-the-art of the major powers probably has some application to electronic warfare. To this may be added information about aerodynamic and astronautic capabilities which interact strongly with electronic warfare capabilities. Beyond this it is up to the inductive and deductive capabilities of the reader to draw the correct conclusions.

The following bibliography is merely suggestive of some of the sources of information about the electromagnetic conflict. To these publications one must include the big metropolitan newspapers, such as the New York Times and the Washington Post, since occasional non-technical items relating to electronic warfare will appear therein.

MAGAZINES

Aviation Week and Space Technology: A weekly covering the entire field of aviation and space with a news magazine approach. This magazine is undoubtedly the best single source of unclassified information about aviation and electronics, including electronic warfare. For example, in 1969 a 4-part series on electronic warfare was carried in these issues: August 25, September 1, September 8, and September 15. In 1971 the 5 issues starting October 4 (October 11, 18, 25 and November 8) contained a series of articles on the Soviet threat. And the February 21, 1972 issue contained a special report on electronic countermeasures.

Electronic Warfare: The official publication of the Association of Old Crows (PO Box 19127, Washington, DC, 20036). It contains articles of current interest to those in the electronic warfare field in all the services. The "Old Crows" are individuals interested in electronics and, specifically, in electronic warfare.

IEEE Transactions on Aerospace and Electronic Systems: This bimonthly technical journal contains many articles on radar which form a good background for electronic warfare. For example, the April, 1961 issue of its predecessor, *The IRE Transactions on Military Electronics* is devoted to radar and contains basic discussions of many of the current radar techniques. Although some articles in this journal can be heavy going for even the experienced engineer, others of the articles are non-mathematical enough to be understandable to the technically-oriented officer.

IEEE Spectrum: This basic journal of the IEEE addresses a wide variety of technical specialties, thus its articles are often of a tutorial or non-mathematical nature. Occasionally, historical articles on the Second World War are printed such as the following three articles by Gordon D. Friedlander:

World War II Radar: The Yellow-Green Eye, Vol 3, No 5, May 1966, Page 62.

World War II: Electronics and the US Navy–Radar, Sonar, Loran, and Infrared Techniques, Vol 4, No 11, November 1967, Page 56.

World War II: Electronics and the US Navy–Magnetic Mines, Acoustical and Homing Torpedoes, and Proximity Fuses, Vol 4, No 12, December 1967, Page 46.

Microwaves: A technical journal whose major emphasis is electronics technology above 100 MHz. It sometimes has ECM related articles, for example, the November 1969, May 1970 and December 1970 issues.

The Navigator: Although the primary thrust of this magazine is aerial navigation techniques and applications, it also carries articles on electronic warfare, since an Air Force officer must be a rated navigator to train as an electronic warfare officer.

Space/Aeronautics: This magazine gives a semi-technical coverage of the aviation and space community with major orientation toward the space community as opposed to the commercial aviation orientation of Aviation Week. Its articles are longer and cover their subject in greater depth than Aviation Week. Occasional articles bearing on ECM will appear.

BOOKS

AF Manual 11-1. *Communications Electronics Terminology*, Volume III. 20 March 1970.

JCS Pub 1. *Dictionary of United States Military Terms for Joint Usage*. Washington, DC: Joint Chiefs of Staff, 1 August 1968.

Technical content is not to be expected of a dictionary, but standardized definitions do abound. The major problem is that a constantly changing field refuses to be bound by standardized definitions, so that there may be conflict between the operators and the definers.

AF Manual 51-3. *Electronic Warfare Principles*. 15 September 1970.

This latest revision of an Air Force manual is very well illustrated and very up-to-date. It concentrates more on the technical details of the electromagnetic conflict than we have done, but the information is presented without a lot of mathematics so that the non-technical reader should be able to understand it. It complements this book very well.

Carroll, John M. *Secrets of Electronic Espionage*, New York: E. P. Dutton, 1966.

A book not well-documented, so some of the very interesting material must be taken with a grain of salt.

Dulevich, V. Ye. et al. *Teoreticheskiye Osnovy Radiolokatsii*, Wright Patterson AFB, Ohio: Foreign Technology Division, FTD-HT-67-192, 22 November 1967.

This machine translation (with English title *Theoretical Fundamentals of Radar*) of the Soviet textbook published in 1964 appears to be about the same level as Skolnik's 1962 book, but with a greater military orientation. It devotes a chapter to active interference (ECM), one to passive interference (clutter) and one to passive location (passive detection).

Gramont, Sanche de. *The Secret War*. New York: G. P. Putnam's Sons, 1962.

A collection of stories of intelligence operations including that of Powers and the U-2, and of the defection of Martin and Mitchell from the National Security Agency.

Hudson, Richard D., Jr. *Infrared Systems Engineering*. New York: John Wiley & Sons, 1969.

A very readable book on infrared which very strongly emphasizes the systems aspect. Thus it is more than a collection of data on infrared, showing the influence of the subjects discussed on systems. A further feature is an annotated bibliography containing topics such as "Search, Track, and Ranging Applications" and "Infrared Countermeasures".

James, Admiral Sir William. *The Code Breakers of Room 40*. New York: St Martin's Press, 1956.

This book has also been published as *The Eyes of the Navy* by Methuen & Co. of London. It is the story of Admiral Sir William Hall, Chief of British Naval Intelligence during World War I. Its style is terse and requires a good familiarity with British Naval history to understand all the action. However, in the fabric of intelligence one can discern the seeds of the modern electromagnetic conflict.

Kahn, David. *The Codebreakers, The Story of Secret Writing*. New York: The MacMillan Company, 1967.

An encyclopedic coverage of cryptology from its earliest inception to the present. Its 970 pages of text are too much to be devoured at one sitting, but the style is quite readable and the documentation is very good. The techniques discussed are illustrated with examples so that the reader gains some comprehension of the ideas involved. The author also does a good job of extracting a fair amount of information about certain not-well-known government agencies from very sparse data.

Pali, Alexander I. *Technik und Methoden des funkelektronischen Krieges*. Berlin: Deutscher Militärverlag, 1968.

This book is apparently a translation (with some editing) of a Soviet Book RADIO-VOYNA published in 1963 by the Ministry of Defense of the USSR. The greater part of the book is devoted to the equipment used for electronic intelligence, electronic countermeasures and electronic counter-countermeasures. There are also sections on the methods of electronic warfare, the history of electronic warfare and electronic espionage. The book is reasonably well illustrated with many illustrations being of western equipment. The book has been translated into English and can be obtained by qualified individuals from the Defense Documentation Center, Cameron Station, Alexandria, VA as document AD 860660L, *Electronic Warfare Equipment and Methods*.

Price, Alfred. *Instruments of Darkness*. London: William Kimber, 1967.

The electronic warfare efforts of the British are described 25 years after their occurrence. The book is interesting reading and illustrates the breadth of effort encompassed by electronic warfare even in World War II.

Schlesinger, Robert J. and others. *Principles of Electronic Warfare*. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1961.

This book on the electromagnetic conflict is currently out of print. It provides technical information at a level which can be understood and used by most students. The book is written to acquaint the electronic warfare specialist with the fundamental technical principles which underlie electronic warfare. It attempts to lay the foundation for the mathematical optimization of aircraft mission effectiveness using ECM. It does not address the problem of how to obtain reliable data with which to perform the optimization.

Shibayev, N. F. *Antimissle Warfare*. Translated by Daniel Wolkonsky, Washington, DC: Aerospace Technology Division, Library of Congress. ATD Report 66-41, 18 April 1966.

This translation of *Borba C raketami* published by Voyennoye izdatel'stvo ministerstva oboroni SSSR, discusses the missile weapons of the main capitalistic countries. Topics discussed include surface-to-surface missiles, satellites, air-to-surface

missiles, air-to-air missiles, surface-to-air missiles, and anti-missile systems.

Skolnik, Merril I. *Introduction to Radar Systems.* New York: McGraw-Hill Book Company, 1962.
This book is a standard reference work on radar with extensive bibliographies. The technical content is of moderate difficulty, but the mathematical developments are minimal so that it is useful to non-engineers.

Skolnik, Merrill I. *Radar Handbook.* New York: McGraw-Hill Book Company, 1970.
A quick characterization of this book is that it is his 1962 book expanded 3 times in size and cost. In the expansion much greater detail has been added so that the character of the book has changed. If you want detailed information on radar this is the book to use. If you need only a good general understanding of radar, the 1962 book is better and cheaper.

Vakin, S. A. and Shustov, L. N., *Osnovy Radioprotivodystviya i Radiotekhnicheskoy Rqzvedki.* Moscow: Izdatel'stvo "Sovetskoye Radio", 1968.
This book is available from the National Technical Information Service, US Department of Commerce, Springfield, VA, as FTD-MT-24-115-69, *Principles of Jamming and Electronic Reconnaissance.* It appears to be the Russian equivalent of Schlesinger's book referenced above. The machine translation is quite readable although the awkard expressions resulting from some of the technical terms makes the mathematics a bit hard to follow at times. In any event, this book provides a look at electronic warfare through a different pair of eyes.

Wolfe, William L. *Handbook of Military Infrared Technology.* Washington, DC: Office of Naval Research, 1965.
This is exactly what the title states, a handbook. It contains voluminous data and is undoubtedly useful to the active worker in the field. However, it yields almost no information about specific systems.

APPENDIX A

ELECTROMAGNETIC WAVE PROPAGATION

Basic to the problem of electronic warfare is the problem of being able to transmit or receive radiated electromagnetic energy (radio waves). In most EW situations either the transmitter or the receiver is in the atmosphere; the ability of the energy to be propagated through the atmosphere is therefore of prime concern. Table 36 summarizes the electromagnetic wave propagation characteristics in the atmosphere for various frequency ranges and .Figure 71 summarizes the US and Soviet frequency band nomenclature.

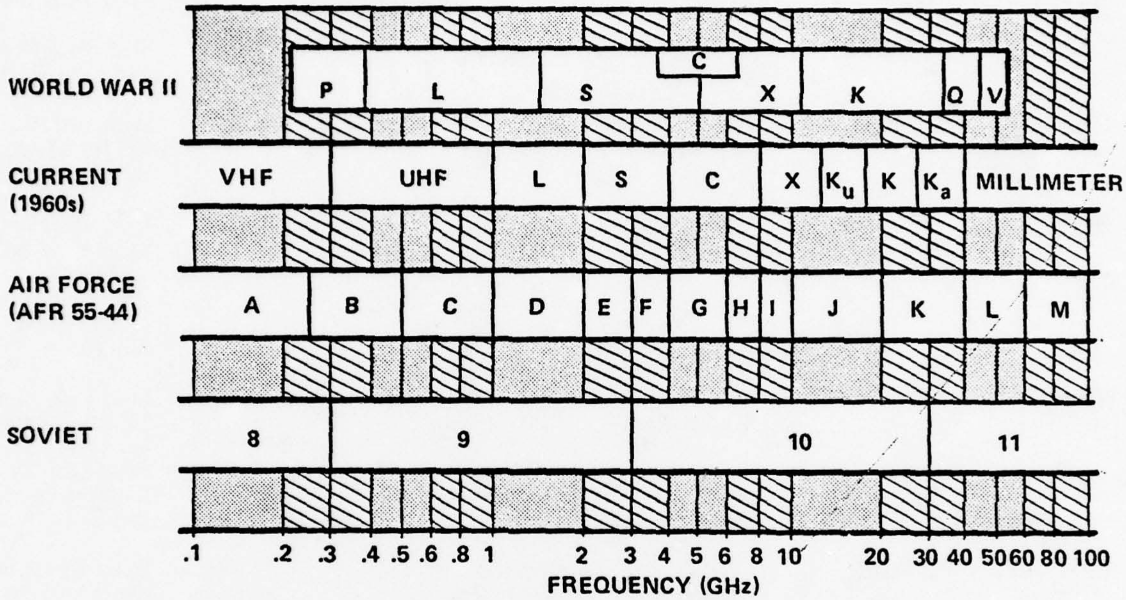


FIGURE 71. FREQUENCY BAND DESIGNATORS

Free-Space Propagation

The *standard used in all discussion of* electromagnetic wave propagation is free space propagation, that is, propagation in a vacuum. Since radio waves and light are both electromagnetic waves, their propagation characteristics in a vacuum are identical; viz., the waves travel at the speed of light in straight lines. In diffuse, un-ionized gasses, radio wave propagation very closely approximates free-space propagation. Thus near the surface of the earth, one has essentially free-space propagation if a straight line connecting the transmitting and receiving antennas encounters no obstructions. This mode of propagation is often called *line-of-sight* (LOS) propagation.

Atmospheric Propagation

As far as radio wave propagation is concerned, the important properties of the atmosphere are the electric and magnetic properties of its molecules. For this reason we divide the atmosphere into five layers as shown in Figure 72. Of these five layers only the Ionosphere and Troposphere have a significant effect on radio wave propagation.

Table 36

Electromagnetic Wave Propagation Summary

Frequency Band	Frequency	Primary Methods of Propagation	Typical Maximum Distance[1,2] (Nautical Miles)	Maximum Message Bandwidth	Use[2]
Very Low (VLF)	3-30 KHz	Ground Wave	5000	50 Hz	Radio Navigation Long Dist. Comm.
Low (LF)	30-300 KHz	Ground Wave Sky Wave	1000-5000	1000 Hz	Med. Dist. Comm. Radio Navigation
Medium (MF)	300-3000 KHz	Ground Wave Sky Wave	100-1000 1000-3000	5 KHz	Med. Dist. Comm. AM Broadcasting Radio Navigation
High (HF)	3-30 MHz	Ground Wave Sky Wave	10-100 100-250 (1 hop) 100-1200 (>1 hop)	5 KHz	Long Dist. Comm. Short Wave Broadcasting Over-the-horizon Radar (OTH) Amateur
Very High (VHF)	30-300 MHz	Scatter Line-of-Sight	600-1200 100 (comm.) 300 (radar)	10 KHz 6 MHz	Long Dist. Comm. TV & FM Broadcasting Short Dist. Comm. Radio Navigation Radar
Ultra-High (UHF)	.3-3 GHz	Scatter Line-of-Sight	30-400 100 (comm.) 300 (radar)	10 MHz 50 MHz	Short Dist. Comm. Radio Navigation Radar
Super-High (SHF)	3-30 GHz	Line-of-Sight	100 (comm.) 300 (radar)	50 MHz	Short Dist. Comm. Radar
Extremely-High (EHF)	30-300 GHz	Line-of-Sight	100	500 MHz[4]	Experimental
Infrared (IR)	1-400 THz[3]	Line-of-Sight	5[5]	10 MHz 10 GHz[4]	Passive detection Lasers
Optical[6]	400-800 THz[3]	Line-of-Sight	0-100[5]	1 MHz 1 THz[6,7]	Lasers Precision Measurement Holography

[1] In the atmosphere. In space, propagation distance is limited only by transmitter power and receiver sensitivity.

[2] "Comm." is a common abbreviation for communications.

[3] Terahertz or 10^{12} Hertz.

[4] Theoretical. It is not known if these bandwidths have been achieved experimentally.

[5] These values are dependent upon the weather conditions.

[6] Coherent light, which is the equivalent of the single frequency oscillator used in the lower bands.

[7] Experimental.

AD-A065 453 AIR FORCE ACADEMY COLO F/G 17/4

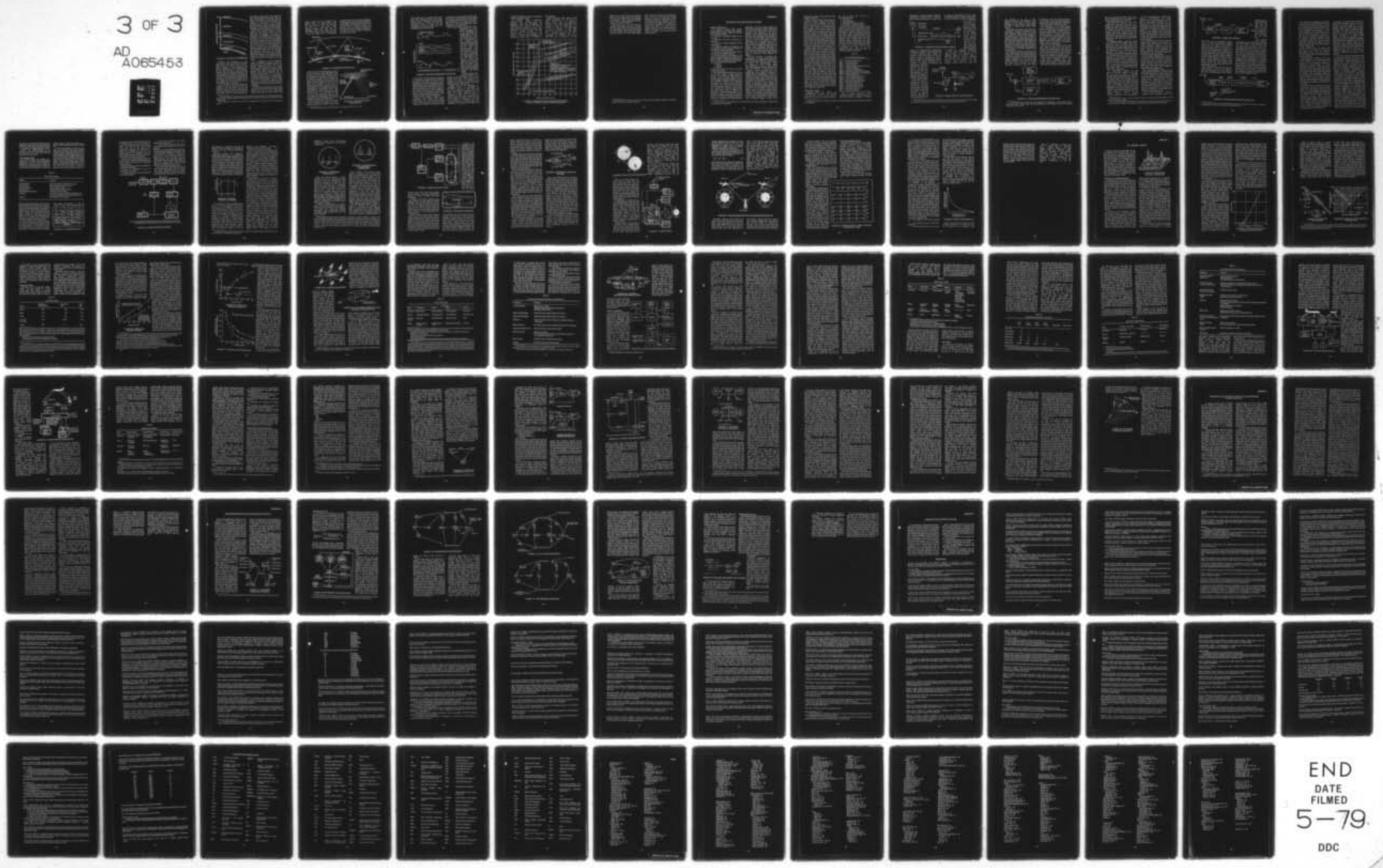
THE STRATEGY OF ELECTROMAGNETIC CONFLICT,(U)

FEB 79 R E FITTS

UNCLASSIFIED NL

3 OF 3

AD
A065453



END

DATE
FILMED

5-79

DDC

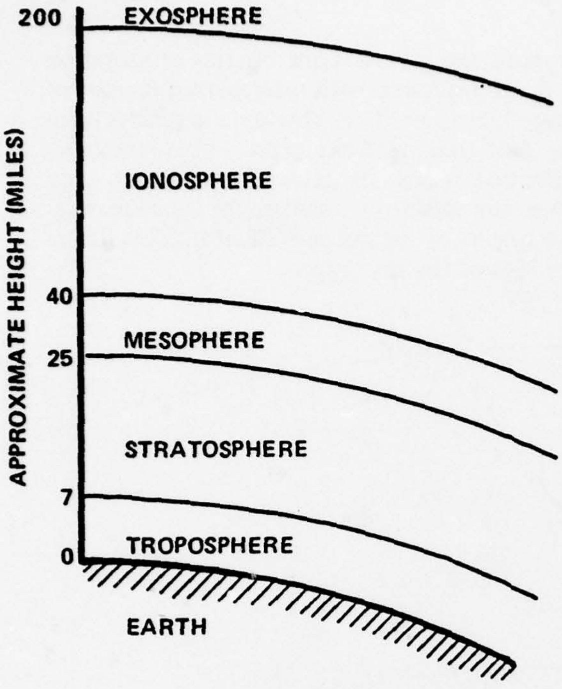


FIGURE 72. THE EARTH'S ATMOSPHERE

Ionosphere. The ionosphere is a very diffuse layer of gas lying between 25 and 200 miles above the earth's surface which is heavily ionized by solar radiation. The primary component of the sunlight responsible for this ionization is the ultraviolet sunlight. however, other components of the solar radiation do contribute, including the atomic particles ejected by sunspots. Thus the ionization of the ionosphere is greatest during the mid-day and least near midnight, but it also changes with the seasons and with the sunspot cycle (an 11 year cycle).

In the ionosphere the solar radiation has stripped one or more electrons from the gas molecules with the result that the gas becomes a *plasma*.[1] When an electromagnetic wave passes through the plasma, the electric field exerts a force on the charged particles and tends to move them. The amount of motion depends upon the particle's charge, its mass, the strength of the field, and the rapidity with which the field changes (the frequency). Any motion of the particle extracts energy from the wave with the result that radio waves traveling through a plasma experience an attenuation due to absorption.

Every plasma is characterized by a critical frequency, the *plasma frequency*, above which the particle motion, and thus the attenuation, is negligible. The situation is analogous to the cutoff frequency of a simple RC circuit, or to the fact that when driving through the mountains the car body follows the road as it goes up and down the hills but that the body moves very little when the car goes over washboard. In the ionosphere the plasma frequency is due to the free electrons, since they have the least mass, and it occurs in the frequency range of 5 to 30 MHz, depending upon the amount of ionization. Below this frequency the ionsphere absorbs, reflects and refracts radio waves; above this frequency it has only a minor effect on the waves.

As a consequence of the ionospheric plasma, atmospheric propagation below the critical frequency takes place between two partially conducting planes: the earth's surface and the ionosphere. The radio waves are essentially trapped in this region and the distance over which propagation can be achieved depends upon how the wave is introduced into this region, i.e. the antenna.[2] Conversely, propagation to a satellite within or outside of the ionosphere is very difficult below the critical plasma frequency. (The existence of a plasma around the satellite is responsible for the communications blackout on reentry.)

Traditionally, propagation below the critical frequency has been explained in terms of the *ground wave* and *sky wave*. Both terms describe the radio wave trapped between the

[1] The major distinction between a plasma and an ionized gas is that the plasma is, on the average, electrically neutral. Thus in the plasma, although the individual particles are charged, the total positive charge equals the total negative charge.

[2] This situation is very similar to the concept of waveguides which is extensively used in the microwave region.

earth's surface and the *ionosphere*. The ground wave is a radio wave which hugs the surface of the earth while the sky wave is a radio wave which bounces between the earth and the ionosphere, often several times. The sky wave only occurs in the region between 1 and 30 MHz and it conveniently explains the fact that one obtains propagation at great distances, with interspersed regions of no propagation. This phenomena results from the fact that near the critical frequency the reflection (due to refraction) occurs only when the radio wave strikes the ionosphere at low angles of incidence.[3] Figure 73 illustrates the idea of the sky wave.

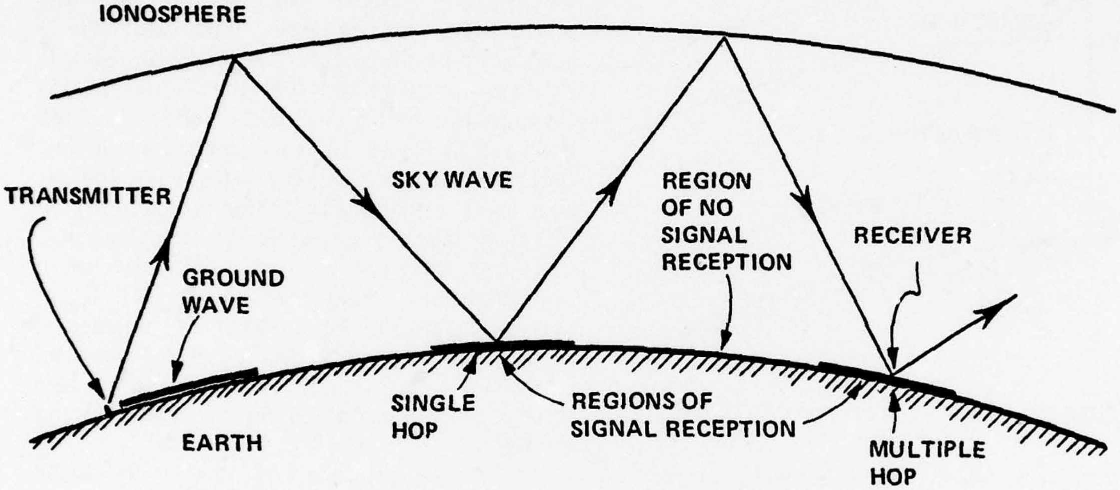


FIGURE 73. ATMOSPHERIC PROPAGATION

More recently the phenomenon of *scatter* has been discovered. This propagation mode occurs just above the critical frequency when the ionosphere is composed of several layers of different densities and the number of layers and their density varies with time and position. The inhomogeneity results in a small signal being returned to the earth at frequencies above that at which the sky wave exists (Figure 74). This signal can be used for communication. An analogous effect occurs while driving at night when one can often determine that a car is approaching before it can be seen (over the crest of a hill, for example) by observing the *forward scatter* of the light from its headlights. The scattering medium in this example is dust or fog.

Because the sky wave and forward scatter *involve* propagation through an inhomogeneous plasma, one frequently observes that

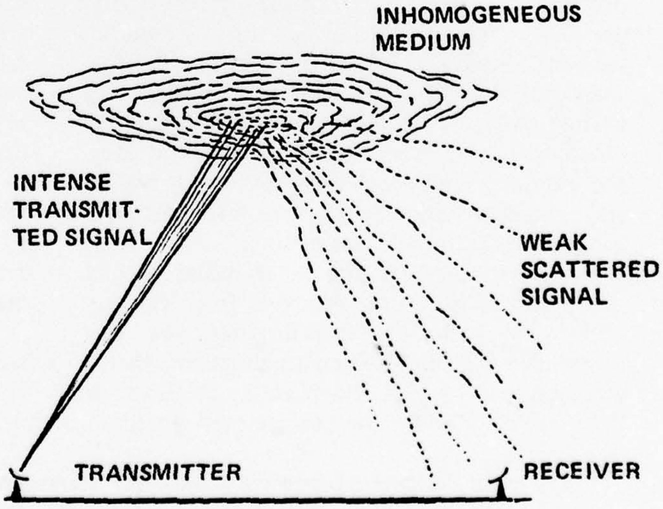
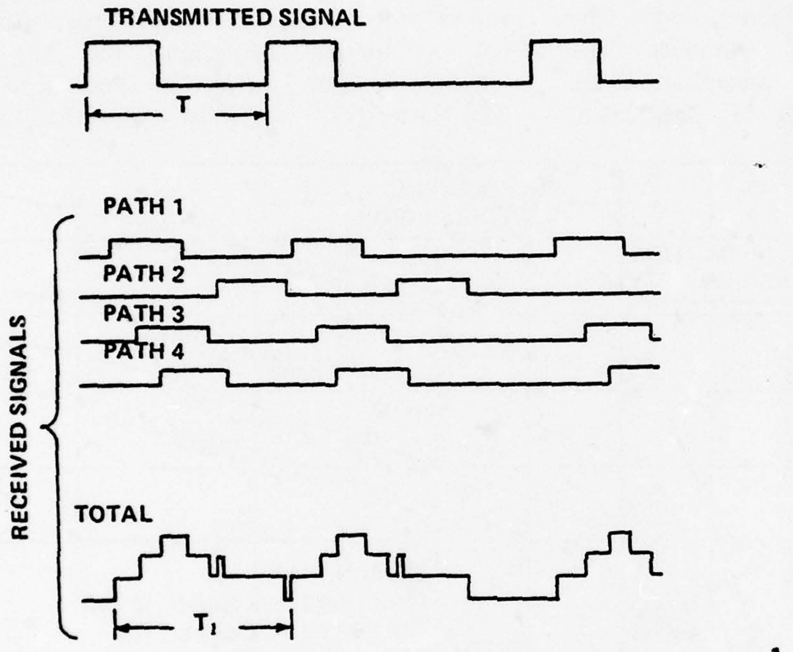


FIGURE 74. FORWARD SCATTER PROPAGATION

[3] The situation is analogous to the reflection seen off the highway ahead on a hot sunny d

several paths exist, a situation called *multipath.* More importantly, there can be time delays of up to hundreds of microseconds between paths. As a result, sky wave and ionospheric scatter are subject to rapid fluctuations in signal strength and to a bandwidth limitation (Figure 75).



FOR UNAMBIGUOUS RECEPTION $T_1 < T$ OR BANDWIDTH $< \frac{1}{T_1}$

FIGURE 75. MULTIPATH BANDWIDTH LIMITATION

Troposphere. The troposphere is composed of a neutral gas; however, because of weather phenomena, the density of the gas is not homogeneous. These inhomogeneities support a reliable scatter mode of propagation in some VHF and UHF bands. This scatter mode also exhibits multipath effects but the spread in time delays is at least 3 orders of magnitude less than that of ionospheric scatter, consequently the bandwidth of this mode is much greater than that through the ionopshere.

There is also a change in density in the troposphere with altitude. This density gradient gives rise to a *refraction* or bending of the radio wave paths toward the earth. Although the bending is not normally enough to return the wave to the earth, it does extend the horizon by about 30 percent. This effect is commonly accounted for in radar line-of-sight calculations by increasing the earth's radius by 1/3, thus many calculations will be specified for a *4/3 earth radius.*

The 4/3 earth radius is commonly used in calculations of tropospheric propagation due to its convenience in determining the RF line-of-sight range. It is, however, based upon a constant vertical gradient of the refractive index above a smooth earth and provides an average value only. The correct value depends upon local meteorological conditions. Thus the use of the 4/3 radius to determine the radio horizon is only an approximation and may not yield correct results if precise path calculations or measurements are required. The more accurate method depends upon knowledge of the local atmospheric conditions and terrain profile.

During certain atmospheric conditions it is possible for sufficient refraction to occur to greatly extend the radio horizon. This condition is known as *superrefraction* or *ducting* and can result in radar line-of-sight ranges two to four times normal.

Another effect of the troposphere on propagation occurs at frequencies in the SHF region and above where the electric and magnetic characteristics of the water and oxygen molecules result in absorption of radio waves in certain frequency bands. The result is that there exist certain *windows* (frequency bands) in which the absorption is minimum and these windows become the preferred bands for propagation. Consequently most SHF and IR systems are designed to operate at frequencies which fall in these windows.

In addition, *visible precipitation*, especially rain, interferes with propagation when the wavelengths are sufficiently small because the solid or liquid particles scatter the waves. Thus propagation in the SHF band and above can be severely affected by the weather, even in the windows. The effects of windows and precipitation are discussed in more detail in Chapter 8.

An Example

Radio Frequency (RF) signals extend beyond line-of-sight (or 4/3 earth, as noted above) due to diffraction, refraction, and scatter (troposphere). An example of the RF signal loss as a function of range for a 10 GHz signal is shown in Figure 76. This figure shows the losses for: (1) free space; (2) a ducting condition; and (3) a combination of diffraction and scatter. The latter case is shown by the four

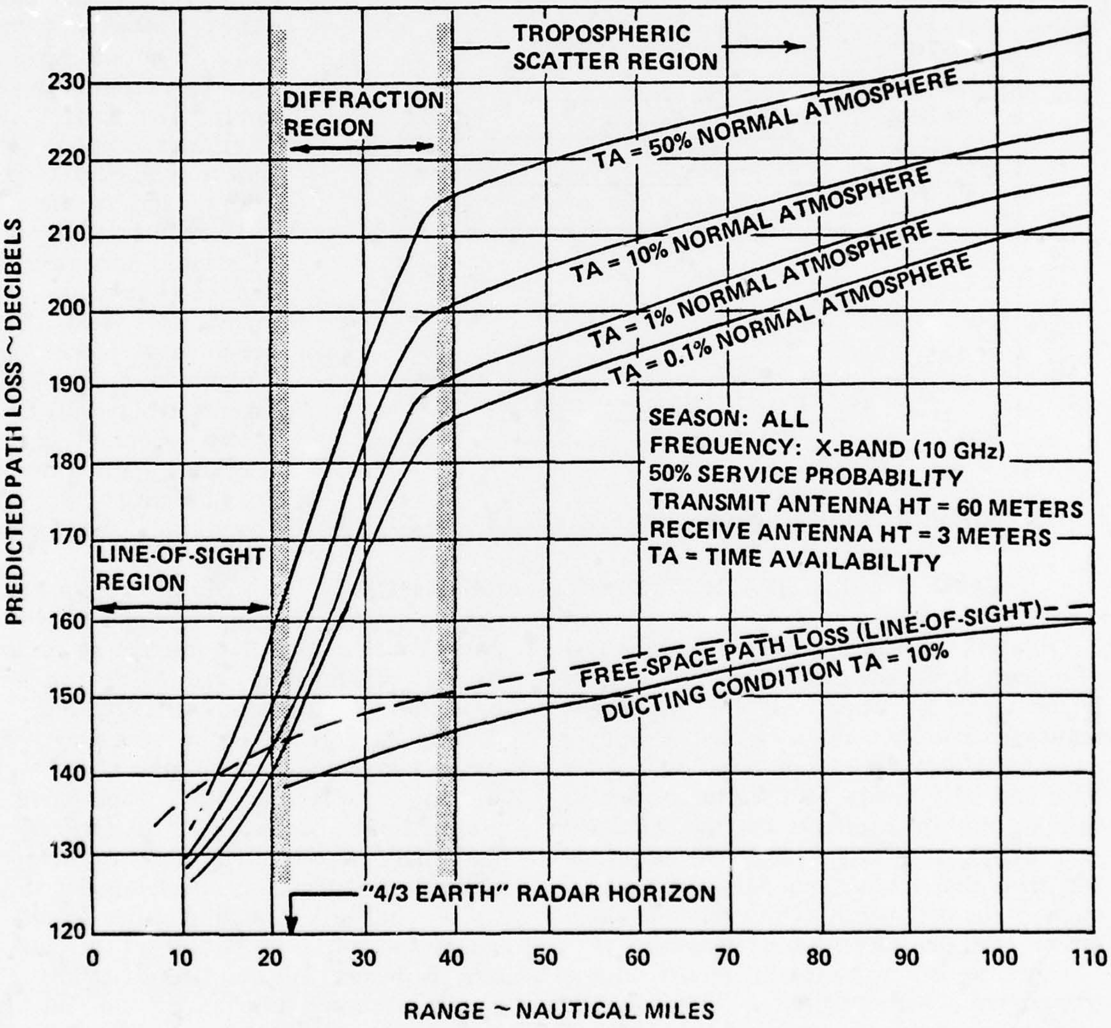


FIGURE 76. PROPAGATION PATH LOSS–WESTERN RUSSIA (DATA FURNISHED COURTESY BOEING COMPANY)

highest curves which provide the predicted path loss for varying time service probability of 50 percent.[4] These curves are dependent upon weather, season, geographical locatión, frequency, and antenna heights.

From Figure 76 it is clear that the transhorizon coverage is broken into roughly the three regions with each region described by the predominant signal transfer mechanism for that region. The line-of-sight region extends to near the 4/3 earth radar horizon where diffraction becomes the predominant factor. At 35 to 40 NM the rate of signal attenuation decreases as tropospheric scatter becomes predominant. Using this data one can determine the signal strength, and hence the detection probability, of a signal transmitted from beyond the radar horizon. Although Figure 76 is for 2 ground stations a similar relationship will hold between an airborne transmitter and a ground based receiving station.

[4] The path loss will be equal to or less than the value shown with a 50 percent reliability for 1/10 percent, 1 percent, 10 percent, or 50 percent of the time.

ELECTRONIC WARFARE RECEIVING SYSTEMS

Receiver Requirements

The electronic warfare (EW) receiver system is designed to intercept many different electromagnetic signals. Ideally, the receiver system should be able to:

1. Intercept a transmitted signal at any frequency.
2. Determine the types of modulation in the signal.
3. Identify the usable intelligence carried by the signal.
4. Accurately measure the direction of arrival of the waveform so that the location of the transmitter can be calculated.
5. Process and preserve the signal characteristics for later in-depth analysis.
6. Provide significant information to the operator (and/or computer) to enable him to make intelligent and timely mission decisions.

This list can be condensed into the generalization that an EW receiver system must:

a. Gather
b. Process
c. Display[1]

all signals of interest to meet its specific mission requirements.

The above requirements are hard to satisfy for the total range of signal parameters involved. For example, no single receiver or antenna system can gather signals over the entire frequency spectrum of interest, usually from 50 MHz to 18 GHz. Yet the surveillance requirements of a mission may dictate that any signal in that entire spectrum be brought to the immediate attention of the operator. This requires many antennas, many tuners, and large display units. In addition, the processing of the intercepted signal may be required to support three different analyses: immediate analysis to determine the potential threat to the collector, immediate analysis to determine if the signal has not been observed previously, and later in-depth analysis for more detailed intelligence content. Depending on their purpose, these analyses will seek to determine such quantities as the center frequency and the side bands of the spectral envelope, the modulation characteristics of the wave form, the signal's scan characteristics, the actual voice, analog, or digital intelligence and the radiated power of the signal. Since it is generally impossible to record the received signal verbatim, one must provide several specialized processors to determine this information and preserve it. Finally that information which is needed for threat warning or immediate signal analysis must be presented to the operators by displays.

The basic approach to meeting these requirements is to make signal collection a four-state process: reception, warning, sorting, and analysis. *Signal reception* uses a receiver to collect the electromagnetic signal and transform it into a form usable for the remaining three states. *Signal warning* alerts the operator to the presence of a signal. It may be provided by audio modulation in the operator's earphones, a flashing light or the presence of a line on a cathode ray tube (CRT). *Signal sorting* often follows immediately upon warning and uses the imprecise warning data about the signal frequency and modulation to sort out the signals of immediate interest. (Signal frequency and modulation usually correlate with the degree of threat each signal presents.) The amount of data presented to the operator depends upon the specific mission requirements, and the amount of equipment that is available. The airborne operator usually has less time and total equipment available than a ground station operator but is more vulnerable to expected threats, so more of his

[1] Display devises are not necessarily a part of the EW receiver, but they are assumed to be part of the receiver system in this appendix.

equipment is designed to perform the warning and sorting function.

Signal analysis includes determining the transmitter's specific capabilities and characteristics for both immediate and future actions. It should not be confused with signal sorting, which usually is to determine only the immediate action required. The current trend appears to be that the airborne data needed for analysis is automatically recorded for later analysis on the ground. Thus the airborne operator concerns himself primarily with signals that present an immediate threat to the aircraft, unusual signals, and signals of great interest that require immediate analysis. As he is able, the operator will also analyze signals and record the results as a backup in case the automatically recorded data is lost.

Because signal analysis is essentially an open-end process (once the signals have been recorded) which can be pursued in relative leisure by ground-based systems, we shall not discuss general analysis further. (The discussion in Chapter 4 gives the general principles of signal analysis.) We shall rather concentrate on the signal reception, warning and sorting functions which must be performed on-board the airborne platform. We shall begin with a discussion of the different types of receivers. Following that we shall discuss the several different displays which are commonly used. Since the signal warning and sorting are performed using these displays, their discussion will encompass the signal processing implicit in these tasks. This discussion will also include the recording function since it is an input to the ground based display used for further analysis. This discussion will merely skim the surface, much more detailed discussions are available in books on receivers and displays or in specialized texts such as that by Pali (See Chapter 10).

Basic Receiver Types[2]

Although many EW systems use superheterodyne receivers, one should not infer that all are of this type. In general, there are four types of receivers, any one of which may be used in a particular application.

1. Crystal video
2. Superregenerative
3. Tuned Radio Frequency (TRF)
4. Heterodyne or Superheterodyne

Each of these receiver types has one basic function, to extract the modulation from the signal. Thus the heart of every receiver is the demodulator or detector. However, there are two general classes of demodulators, those that recover signal amplitude variations and those that recover signal frequency or phase variations. Even though there are many different kinds of modulations, the more common of which are listed in Table 37, these two generic types of demodulators will suffice to recover all of them; however, minor modifications may have to be incorporated before or after the detector to match a specialized modulation.

Table 37

Common Signal Modulations

AM	Amplitude Modulation
DSB	Double Sideband
SSB	Single Sideband
SSSC	Single Sideband Suppressed Carrier
VSB	Vestigial Sideband
FM	Frequency Modulation
WBFM	Wideband Frequency Modulation
NBFM	Narrow Band Frequency Modulation
PM	Phase Modulation
PAM	Pulse Amplitude Modulation
PWM	Pulse Width Modulation
PDM	Pulse Duration Modulation
PPM	Pulse Position Modulation
PCM	Pulse Code Modulation
ASK	Amplitude Shift Keying
FSK	Frequency Shift Keying
PSK	Phase Shift Keying
CW	Continuous Wave

Thus, in general, modulations which incorporate the term frequency or phase in their title require a frequency or phase

[2] Some of this discussion is taken from a student text published by the Technical Training Center, Keesler AFB, Mississippi.

demodulator; all others require an amplitude demodulator, commonly called a detector. Since frequency modulation is much more common in communications applications, frequency demodulators are not widely used in ELINT receivers, which support the majority of EW users. Hence we shall not discuss frequency demodulation further. However, either the Tuned Radio Frequency receiver or the (super) heterodyne can be converted to frequency demodulation by replacing the amplitude demodulator with a frequency demodulator. (The crystal video and superregenerative receivers are only capable of amplitude demodulation by their inherent design.)

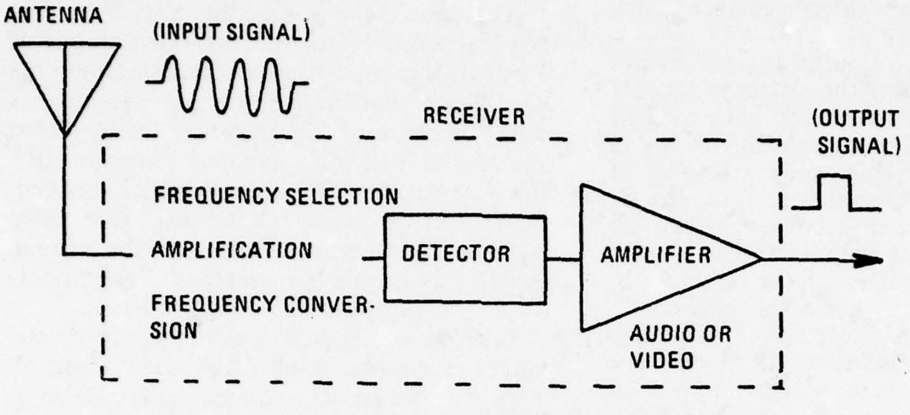


FIGURE 77. THE BASIC RECEIVER BLOCK DIAGRAM

Given that the basic function of a receiver is demodulation, the basic technical problem becomes that of selecting and suitably transforming the signal so that the detector can properly function. This may involve either amplification or frequency transformation or both. Thus the distinction between receivers is the means by which frequency selection, amplification and frequency conversion is accomplished. Hence one might diagram a receiver as in Figure 77 with the contents of the missing portion of the block diagram determining the receiver type.[3] The list of receiver types given above orders the different receivers in order of increasing complexity.

Crystal Video Receivers. A crystal video receiver is the simplest of all receivers since it contains only a frequency selective circuit, or preselector, between the antenna and the detector. The modulation is thus abruptly removed from the carrier and

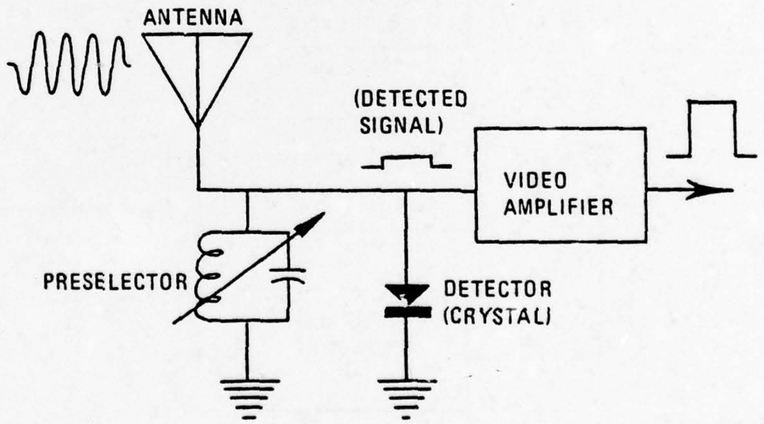


FIGURE 78. A BASIC CRYSTAL VIDEO RECEIVER

[3] The figures of the basic receiver types (Figures 77 through 81) have been annotated with symbolic signal waveforms for a pulse (radar) signal to illustrate the signal processing performed by the circuit.

then amplified by the audio or video amplifier.[4] Usually a video amplifier is used because the RF carrier is often pulse-modulated by short duration pulses. Figure 78 shows a crystal video receiver block diagram.

The frequency selection by the preselector is necessary to restrict the detector to only those signals of interest on the basis of their carrier frequency. The preselector circuit in the diagram is symbolic only (although a lumped parameter, tuned circuit could be employed at the lower RF frequencies), for the crystal video receiver finds its true place in the microwave frequency range where distributed circuits such as coaxial and cavity resonators are used for purposes of frequency discrimination. Furthermore, the preselector may or may not be tunable depending upon the application.

The crystal is typically a microwave silicon diode. This element is the most critical item in the receiver because the receiver sensitivity (its ability to receive weak signals) is almost entirely determined by the crystal. The nominal sensitivity of a microwave crystal (3GHz to 10GHz) is 10^{-8} watt or -50 dBm; this makes for a relatively low receiver sensitivity compared to the other types. Furthermore, since the crystal operates at very low input levels it follows the square-law characteristics, and consequently, linearity is not a feature of the crystal-video receiver.

The nonlinearity of the crystal places unusual requirements on the video amplifier. First, its dynamic range is exaggerated by the square-law characteristic of the detector. A dynamic range of 10^6 in power (or 60 dB) at the crystal calls for a dynamic range of 10^{12} (or 120 dB) in the video amplifier. Second, high gain is required because the video amplifier is the only amplifier in the system. Finally, both of the previous requirements imply low-noise amplification.

Because of its low sensitivity the crystal video receiver is most often used when all signals over a broad frequency range are to be detected. Thus the preselector can be omitted in which case the frequency range is limited only by the antenna. An example of such a system is the AN/APS-54 warning receiver.

These various sections of the crystal video receiver may be integrated into a very compact system. A 10 GHz antenna, tuner, crystal, video amplifier, and power source could easily be packaged in the space required

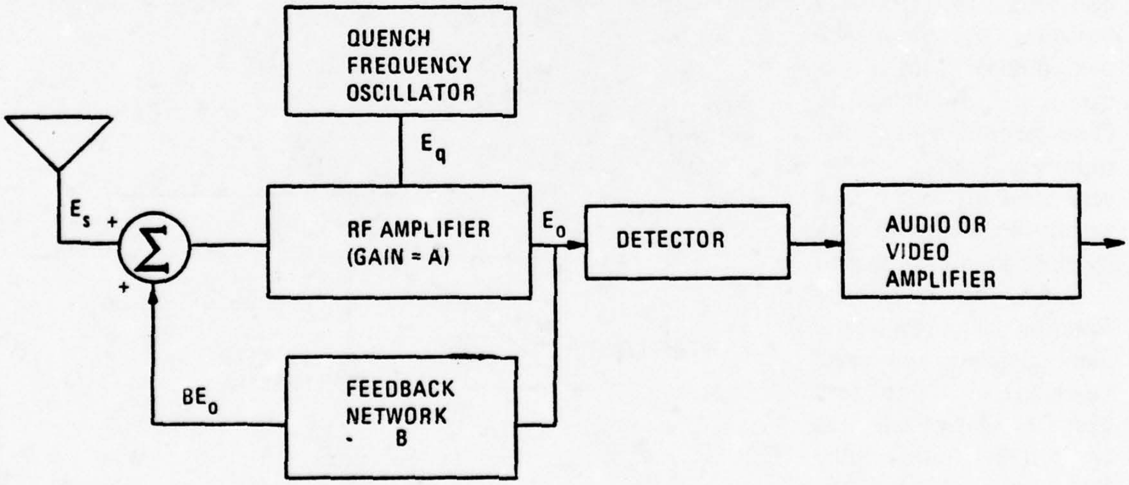


FIGURE 79. A BASIC SUPERREGENERATIVE RECEIVER

[4] The difference between an audio and a video amplifier is one of bandwidth. An audio amplifier has a pass band sufficient only for speech, seldom more than 20-20,000 Hz. A video amplifier commonly has a passband extending to 1 MHz or more.

by a small transistor portable radio. If the PRF to be detected were at an audible rate, a suitable display might be an earphone.

Superregenerative Receivers. The most obvious way to improve the sensitivity is to amplify the signal before detection. If this amplification can be done without increasing the detector noise level, then a net increase in sensitivity will result. Or conversely, if the receiver input noise remains the same, the amplification will not increase receiver sensitivity but it may allow one to use cheaper components with less critical tolerances for the receiver.

The simplest amplifier would be a single active vacuum tube or transistor stage, but at frequencies above 50 MHz it has been difficult to achieve high single-stage gain. The superregenerative receiver, Figure 79, contains an ingenious way of circumventing this difficulty. The portion of the receiver between the antenna and the detector consists of a feedback system in which the output, modified by some feedback network B, is added to the input signal in a positive sense. This added input is, in turn, amplified and fedback so that the output signal continues to grow as the system "chases its tail". Hence there is the potential for large amplification and voltage gains of 120 dB have been achieved in a single stage.

A mathematical analysis of this circuit with positive feedback shows that the net gain is $E_o/E_s = A/(1\text{-}AB)$. As the product AB approaches unity the gain increases without bound and when AB $\geqslant$ 1 the system breaks into oscillation and so becomes blind to any inputs. Thus large gain implies keeping AB just slightly less than unity. For example a gain of only 1,000 requires AB = 0.999 and this value must be maintained within 0.001 percent if any gain stability is to be obtained. The *regenerative* receiver attempts to maintain such gain stability directly but it requires continual adjustment to prevent oscillation.

In the *superregenerative* receiver this problem is circumvented by another approach. The value of B is adjusted to a safe value so that random fluctuations will not drive the circuit into oscillation; then the amplification A is varied at a frequency called the *quench* frequency (much higher than the information or modulation frequency) by means of an auxiliary signal E_q which modulates some parameter of the amplifying device.[5] This fluctuation in A is great enough to allow the AB value to reach and exceed unity for a small fraction of each cycle of the quench frequency.

One interpretation of the effect is that the system passes through the condition of "infinite" gain many times per second (the quench frequency), indeed, at a rate well beyond that which can be discerned by the signal processing devices following the receiver (which may be an individual wearing headphones). The net effect is that of a continuous highly amplified signal.

A more realistic interpretation is that the system breaks into oscillation during the short interval that AB $\geqslant$ 1. When a signal is present it breaks into oscillation earlier in the quench frequency cycle than it does in the absence of a signal. The integrated effect of these pulses is a replica of the modulation envelope of the incoming signal.

The superregenerative principle has no carrier frequency limitations; it has been used in 10 GHz receivers and at audio frequencies. It can be used even at optical frequencies where the amplifier is a laser. Unfortunately it suffers from (1) gain instability, (2) poor selectivity, (3) reradiation,[6] and (4) high noise level, so it is not commonly used. But in those few applications where (1) simplicity, (2) high gain, (3) light weight, (4) small size, and (5) transmit-receive capability are a paramount importance, the superregenerative receiver has a great deal to offer.

Tuned Radio-Frequency Receivers. Another way of increasing the signal level at

[5] Since in general $A = g_m z_L$, it would be possible, for example, to modulate the transconductance, g_m, of the device to obtain a time-varying A.

[6] Because the RF amplifier periodically goes into oscillation and is connected to an antenna the receiver may act like a transmitter, radiating its own signal (not necessarily the same signal as the one being received).

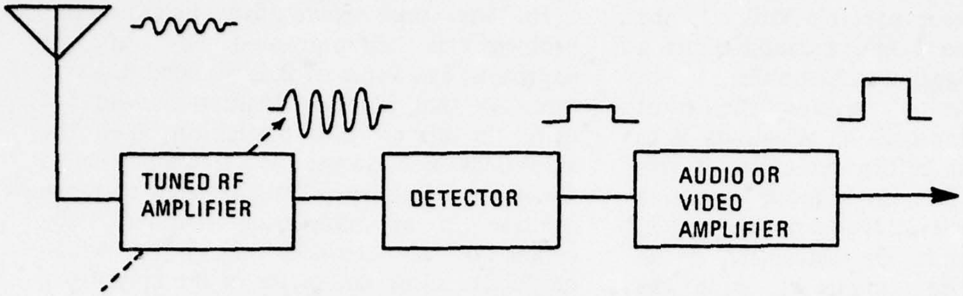


FIGURE 80. A BASIC TRF RECEIVER

the detector is to use a multi-stage amplifier, that is a tuned radio-frequency amplifier (Figure 80). The tuning of the amplifier means that its band-pass is restricted to a small percentage of its center frequency so that the net amplification per stage can be increased. The result of this amplification is that the signal level at the detector is raised to the point where sensitivity no longer depends upon the crystal detector. Further, a series of active, tuned amplifiers provides better selectvity characteristics than a passive, tuned circuit. Finally, the video amplifier gain requirements are much reduced because the detected signal is larger.

The noise factor[7] of a tuned radio frequency (TRF) receiver, in fact of any receiver, is determined primarily by the first amplifier. Thus the noise performance of this receiver depends upon the design of the first stage. Since this stage does not have to provide all the gain as in the superregenerative receiver, it can be optimized for low noise level.

The crucial point of TRF receiver design is to develop enough stable gain in the RF amplifier to take advantage of the low noise factor. Because of the short wavelengths (high frequencies) involved even short lengths of wire act as antennas and it is very easy to have parasitic, positive feedback around any or all the stages of the amplifier. Thus it is often impossible to isolate the input of the amplifier sufficiently well from its output to prevent regeneration of the signal. Such regeneration invariably leads to disabling oscillation in the RF amplifier. A commonplace example of this type of behavior is found in the case of a powerful public-address amplifier with a poorly located microphone. The regeneration of the output signal which results when a small fraction of sound from the loudspeaker enters the microphone often leads to uncontrollable howling.

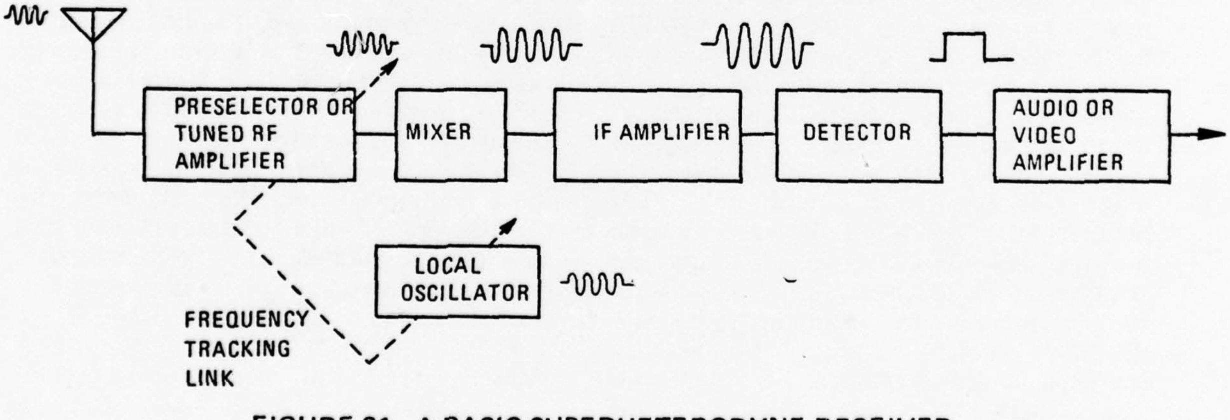


FIGURE 81. A BASIC SUPERHETERODYNE RECEIVER

[7] Noise factor is a measure of the extra noise added to a signal by an amplifier. It is the ratio of the noise with the amplifier present to the noise in the signal with the amplifier absent.

The solution to the problem for the TRF receiver is to add sufficient negative feedback or *neutralization* around each stage to cancel the parasitic positive feedback. This solution is very straightforward and adequate as long as the amplifier center frequency is fixed (fixed-tuned). But a common requirement is that the center frequency be varied over a wide range, so that the neutralization, which is frequency dependent, becomes almost impossible to insure over the total tuning range. Thus TRF receiver design is often a tradeoff between great sensitivity (high gain) and wide tuning range.

TRF receivers may be used at all frequencies. At low frequencies, conventional RF amplifiers are used. At microwave frequencies one may use such devices as a low-noise traveling-wave tube (TWT) amplifier for the rf amplifier.

Superheterodyne Receivers. The most common approach to transforming the signal at the antenna into a form suitable for detection is to use frequency conversion to translate the received signal to a fixed intermediate frequency. At this intermediate frequency a fixed tuned, neutralized, amplifier (IF amplifier) provides both the gain and the frequency selectivity desired. The change in frequency also discourages regeneration because the signal at the detector is not the same frequency as that at the antenna. However, the frequency changing operation also adds spurious frequency responses which can hinder the operation and calibration of the receiver.

The block diagram of Figure 81 shows the organization of a typical superheterodyne receiver. The preselector may be a passive filter or an active amplifier depending upon the design. Strictly speaking, if the preselector is a passive filter the receiver is called a *heterodyne* receiver, while the term *superheterodyne* implies that the preselector is an rf amplifier. However, in common usage, either version is called a superheterodyne. In either version the function of the preselector is to decrease and ideally eliminate the spurious frequency responses introduced by the frequency conversion operation.

The mixer, also called the *first detector* is the frequency converter. Its basic action is to multiply the received signal by a locally generated signal, the signal from the local oscillator; with the result being two signals containing the original modulation whose frequencies are the sum and the difference of the received and local oscillator signals. Typically in a correctly tuned receiver the different frequency is the IF frequency, hence it is accepted and amplified by the fixed-tuned IF amplifier, and all other frequencies are rejected. Since the IF frequency is fixed, a moments reflection will show that tuning must be accomplished by changing the local oscillator frequency. The preselector must also be tuned but its bandpass is large and its gain is relatively small, so tuning does not present a great problem.

It is in the fixed-tuned IF amplifier where the frequency selectivity and gain of the superheterodyne receiver are located. If the required gain is greater than can be easily obtained with a single IF amplifier, then additional frequency conversions can be made. This multiple conversion receiver will have as many different IF amplifiers as it has frequency conversions. Unfortunately the number of potential spurious frequency responses equals 2^n-1 where n is the number of frequency conversions, thus a large number of frequency conversions implies a high potential for uncalibrated responses unless a considerable design effort is put forth. For example, a receiver tuned to 1,000 MHz might use a first IF amplifier with a 260 MHz center frequency, followed by a converter and second IF amplifier with a 140 MHz center frequency, followed by a final coverter and third IF amplifier with a 40 MHz center frequency. The cascade may produce an extremely large gain but regeneration is prevented because the 40 MHz output signal will not be accepted by the input which is tuned to 1000 MHz. But this cascade could have 7 spurious frequencies: 1280, 1200, 1080, 480, 400, 280, and 200 MHz. And if the receiver is not well shielded, so that strong signals can penetrate to the second and third frequency converters (also called second and third mixers or second and third detectors) responses at 540, 460, 340, 260, 140, 60 and 40 MHz are also possible. Thus good design is very important in superheterodyne receivers.

Because the superheterodyne is so common, we will adopt the viewpoint that all EW receivers are of this type for the remainder of our discussion.

Receiver Display Units

As described before, the function of a receiver is to intercept the electromagnetic transmission at some specific frequency, separate the modulation and reproduce the modulation in some usable form. As ideal EW receiver would have the ability to receive and display signals simultaneously over the entire frequency spectrum but this is not practical. As many items of information are required to analyze an intercepted signal, manv types of display units have evolved. The most common displays used in EW receiving systems are listed in Table 38. The number of these displays included in a particular aircraft will depend on its mission; the reconnaissance position in an ELINT collector may have all seven while a fighter may have only two.

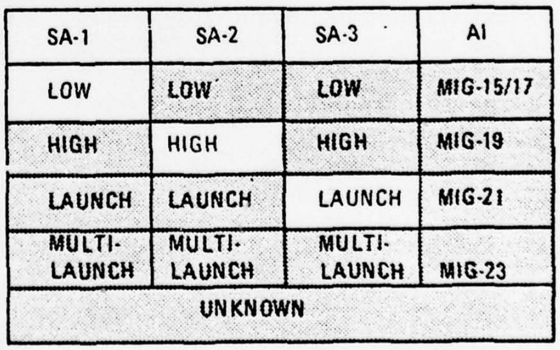
Table 38

EW Receiver Displays

Display	Function
Warning display	Show the presence of high-threat signals
Audio System	Present signal modulation aurally
Panoramic adapter	Display signal spectrum
Pulse Analyzer	Determine pulse width and PRF
Direction finding (DF) unit	Determine relative bearing
Computer	Compute the signal transmitter's geographic location, analyze and identify signal parameters, etc.
Recorder	Save signals for later analysis

Warning Displays. The outputs of specialized receivers, computers or electronic filters are usually coupled to warning lights to form the warning display. Their purpose is to draw the operator's attention to signals that pose a high degree of threat and/or are of special mission interest. Often these lights are in groups (called billboards) as shown in Figure 82.

For the warning displays to be of any value they must perform their signal analysis reliably under all combat signal environments without assistance from the operator. Yet it is obvious that the combat signal environment is very uncertain, thus it is impossible to predict the total numbers and strength of the signals which must be analyzed by the electronic circuits driving the warning lights. Consequently, it is reasonably certain that at some time a combination of signals will occur that the electronic circuits will be unable to analyze. In order for this display to be useful under these circumstances it must be "fail-safe". That is, the operator must have



SA-1	SA-2	SA-3	AI
LOW	LOW	LOW	MIG-15/17
HIGH	HIGH	HIGH	MIG-19
LAUNCH	LAUNCH	LAUNCH	MIG-21
MULTI-LAUNCH	MULTI-LAUNCH	MULTI-LAUNCH	MIG-23
UNKNOWN			

FIGURE 82. A BILLBOARD DISPLAY

the assurance that if the analysis circuits fail the warning will not be lost. There must be some way of telling him that a signal exists which does not fit into any of the programmed categories (the "unknown" of Figure 82). Otherwise, he may turn the warning display off, preferring to do the threat analysis himself to trusting a black box that is silent at the most critical times.

Audio System. Since the human ear is not precise enough for detailed signal analysis the audio system usually serves as an alternate warning system.

The audio warning devices can generally be grouped into two classes:

1. Audio that designates the type of warning (tone or words).

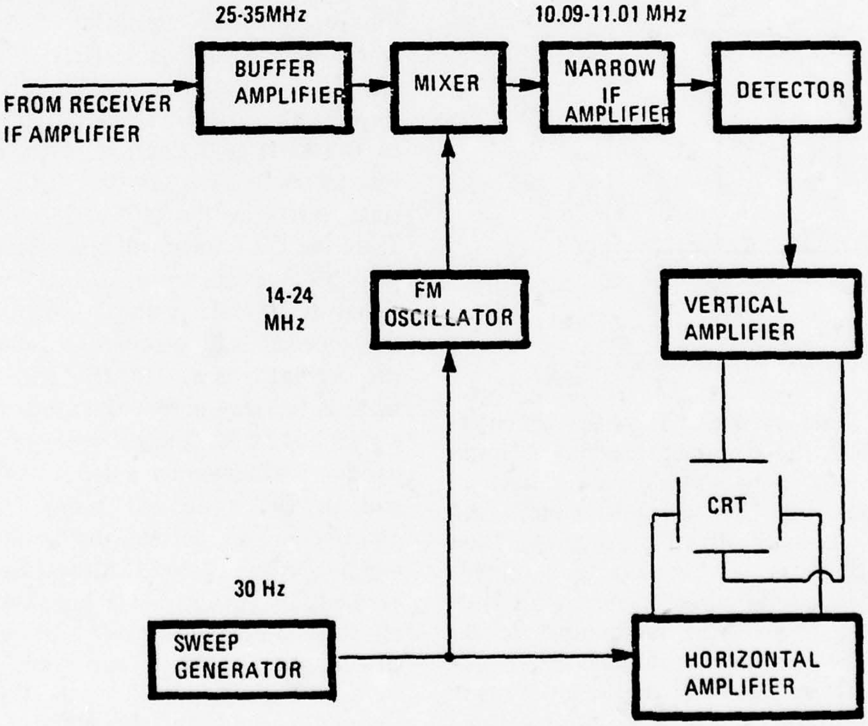
2. Audio tones that give the parameters of the intercepted signal.

a. The actual parameter (the audio signal from the receiver).

b. The synthetic parameter (an audio signal made by the computer as a result of its analysis).

The first class would probably be driven from electronic circuits similar to those which drive a warning display billboard. Likewise synthetic tones in the second class would be generated as a result of signal analysis by similar circuitry. In both these cases the requirement for fail-safe operation applies for the same reasons given under warning display—the operator cannot afford to be ignorant of possible high-threat signals.

In the case where the operator hears the actual demodulated signal from the receiver the fail-safe requirement does not apply because the operator is making the analysis. And although this places more of a load on



NOTE: THE FREQUENCIES GIVEN ABOVE ARE FOR ILLUSTRATION ONLY. THEY ARE NOT INTENDED TO BE COMPATIBLE WITH ANY PARTICULAR RECEIVER SYSTEM.

FIGURE 83. A BASIC PANORAMIC ADAPTER

the operator it is generally true that the human ear-brain combination is less likely to be deceived by new or unusual combinations of signals.

Panoramic Adapter. The panoramic[8] adapter (panadapter) display is an oscilloscope that measures signal voltage amplitude on its vertical axis and frequency in Hertz (instead of time) along its horizontal axis from left to right. The purpose of the adapter is to present a visual indication of all signals within the receiver IF bandpass. The display is driven by signal processing circuits which operate on the signal contained in the receiver IF section. Figure 83 is the block diagram of a panoramic adapter for a superheterodyne receiver whose IF amplifier passband is shown in Figure 84.

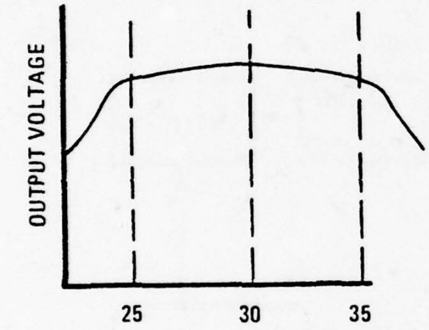


FIGURE 84. A TYPICAL RECEIVER IF BANDPASS

The first stage is a buffer amplifier which is used to isolate the companion receiver from the mixer in the panadapter. It must have a wide bandpass (e.g. 20 MHz) to handle all frequencies within the IF of the receiver. The output of this stage is coupled to a mixer stage which combines these signals with the output of a frequency modulated local oscillator. The frequency of this oscillator periodically varies over a frequency range equal to the usable bandpass of the receiver IF amplifier. The new IF from the panadapter's mixer is passed through a narrowband IF amplifier and coupled to a detector stage. The detected output is then fed through a video amplifier to the vertical deflection plates of the CRT display.

Now let us consider the horizontal sweep channel. A sawtooth waveshape generated by the sweep generator is fed to (1) a horizontal (video) amplifier, and (2) the FM oscillator. The output of the horizontal amplifier is applied to the horizontal deflection plates of the CRT display to generate the display sweep. The same sawtooth voltage is sent to the FM oscillator to change its frequency in synchronization with the sweep. If the sweep generator in Figure 83 produces a 30 Hz sawtooth then each 1/30 second (1) the electron beam moves across the scope, and (2) the FM oscillator frequency varies between 14 MHz to 24 MHz.

Suppose there is a CW signal at 25 MHz in the receiver's IF amplifier at the moment when the FM oscillator starts at 14 MHz; the difference frequency of 11 MHz will pass through the 11 MHz IF amplifier of Figure 83 to the vertical deflection plates and cause a vertical deflection on the CRT just as the trace starts at the left end of the baseline. Thus the CRT trace will be deflected upwards at point A as shown in Figure 85. Similarly a signal at 30 MHz in the 10 MHz bandpass of the receiver will produce a deflection when the oscillator is at 19 MHz and the baseline trace is halfway across the scope face. Finally a signal at 35 MHz in the receiver IF amplifier bandpass will produce a deflection at the right end of the sweep at point C. Thus the panoramic adapter has displayed the signals existing in the IF bandwidth of the receiver as vertical deflections on a linear sweep. Their relative amplitudes and positions along this sweep thus accurately represent their actual appearance in the IF signal frequency spectrum. Since the IF signals have been translated from the RF signals, these signals have the same amplitudes and spacing as the original signals. Hence the display can be

[8] Panoramic is derived from the Greek words *pan* meaning all and *horao* meaning tc gaze intently at. In this context it means to visually present all frequencies.

calibrated in terms of the original signal amplitudes and frequencies, as is portrayed in Figure 85.

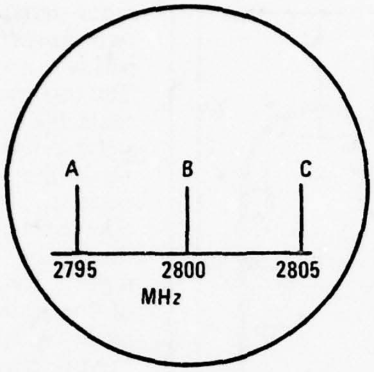


FIGURE 85. A PANORAMIC SCOPE DISPLAY

From this spectral display a trained operator may be able to determine the signal modulation and scan characteristics. For example an estimate of the PRF of a radar signal may be obtained from the spacing of the vertical lines in the display.[9] (A low PRF signal has vertical lines which are more closely spaced than a high PRF signal.) The amplitude of the signal displayed can also be used as an indication of relative received signal strength. Therefore, in Figure. 86 the left hand signal is probably stronger than the right hand signal and its PRF is higher. And if a scanning radar signal is intercepted. It is possible to determine its scan duration with a stop watch or computer.

In summary, the panadapter is an oscilloscope whose horizontal axis is calibrated in frequency instead of time. From its display the operator can obtain the following information: type of modulation, relative intercepted signal strength, scan rate, and approximate PRF.

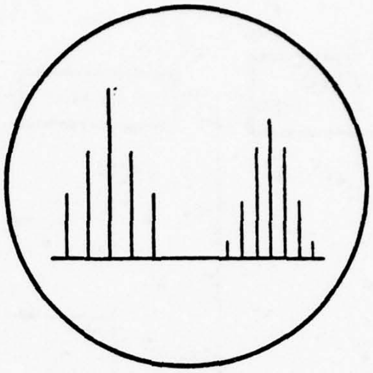


FIGURE 86. THE APPEARANCE OF SIGNALS ON A PANADAPTER

Pulse Analyzer. The electronic pulse analyzer is designed to assist in identifying radars by determining pulse width (PW) and pulse repetition frequencies (PRF). In some analyzers both of these determinations are made by comparing the input signals with calibrated sawtooth sweeps on the face of a CRT. Other analyzers determine PRF by comparing the input signal with the output of a calibrated sine wave oscillator. However, most pulse analyzers resemble the common oscilloscope in that they display signal amplitude as a function of time. The elapsed time is usually displayed from left to right on the horizontal axis of the CRT. We shall consider one that uses two calibrated sawtooth sweeps to display two horizontal displays on the face of one CRT. This is often called a two-gun or multi-gun CRT display.

The simplified block diagram, as shown in Figure 87 illustrates the principles of operation of the pulse analyzer. The pulse input is introduced into a video amplifier which amplifies the weak signal and changes the polarity of the incoming pulse, if necessary, to display an upward deflection on

[9] This discussion has assumed that the panadapter is operated as a spectrum analyzer in the "line" mode where the panadapter bandpass is narrower than the spacing between spectrum lines. This mode implies a slow sweep speed which may be operationally untenable if a wide spectral width must be surveyed. It is possible to operate in a "pulse" mode with a much faster sweep speed and still obtain useful information, but the display is no longer that of the signal spectrum. A good discussion of these two cases is found in *Spectrum Analysis . . . Pulsed RF*, Hewlett Packard Application Note 150-2, (Palo Alto, California: Hewlett-Packard, November 1971).

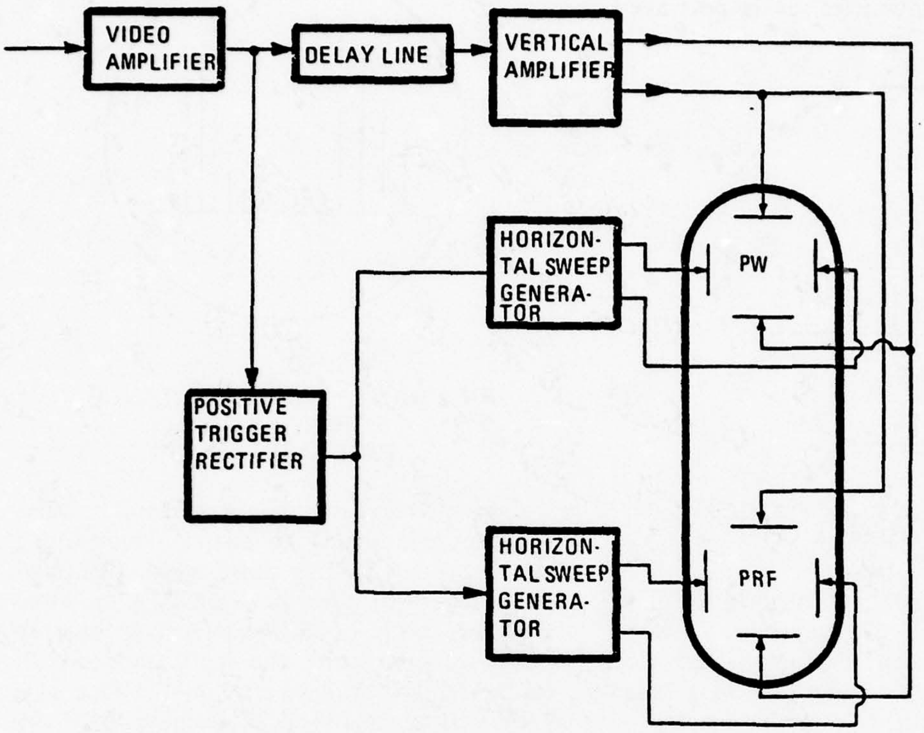

VIDEO AMPLIFIER
DELAY LINE
VERTICAL AMPLIFIER
HORIZONTAL SWEEP GENERATOR
PW
POSITIVE TRIGGER RECTIFIER
HORIZONTAL SWEEP GENERATOR
PRF

FIGURE 87. A BASIC PULSE ANALYZER

the face of the CRT. The video amplifier usually includes a frequency compensation network to preserve the shape of the pulse modulation.

A portion of the video amplifier output passes through the delay line and vertical amplifier to the vertical deflection plates of the CRT. The delay line delays the vertical video pulse to ensure that the horizontal sweep on the CRT has begun before any vertical deflection occurs, thus preventing the loss of any part of the leading edge of the displayed pulse.

Another portion of the video amplifier output is sent to the trigger rectifier where it is differentiated and the negative overshoot is clipped. This produces a narrow pulse which triggers the sweep generators for both CRT guns. The sweep generators' sawtooth outputs are fed to the horizontal deflection plates and the electron beams are swept across the face of the CRT at rates proportional to the slopes of the sawtooth voltages.

Figure 88 illustrates the appearance of the radar signal on the two traces of the pulse analyzer. The top trace presents the received radar pulse width while the bottom trace enables the operator to obtain the pulse recurrence frequency of the radar. The pulse width presentation, top trace, is calibrated in terms of time (microseconds) so it is possible to measure the pulse width directly. For example the pulse displayed in Figure 88 is approximately 4 microseconds long. The sweep for the bottom trace also travels in the same direction as the top trace, if this trace were calibrated in terms of time the lower trace would be 1,000 microseconds long. Since all radar pulses received during this 1,000 microseconds are presented on the trace, the operator could measure the time between two successive pulses and compute the PRF from the formula: PRF = 1/PRT. However, the lower trace of the pulse analyzer in Figure 88

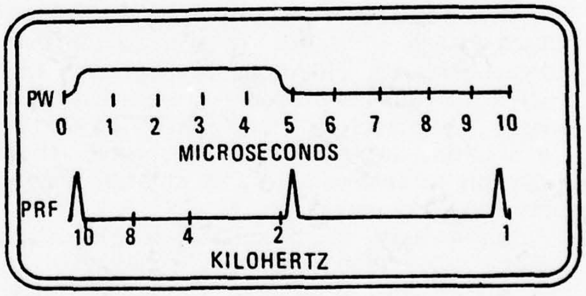


FIGURE 88. A PULSE ANALYZER SCOPE

displays the PRF directly by calibrating a scale in PRF from right to left, in the opposite direction from the sweep. The PRF is then read directly under the second spike from the left side of the scope. A short time between two pulses represents a high PRF while a comparatively long time represents a low PRF.

In Figure 88 a pulse train from a radar with a PRF of 2,000 pps is shown on the PRF trace. Since the second pulse from the left occurs 500 microseconds later than the first pulse (halfway across the trace), the PRF of the signal is read on the scale as 2,000 pulses per second. Thus the pulse analyzer allows the operator to quickly determine the PRF and pulse width of a radar signal.

Direction Finding Unit. If enemy electronic weapons are to be neutralized, it is important that their locations be known in order that the countermeasures will be used in the proper area. The equipment that locates the sites is referred to as the direction finding (DF) unit. A basic direction finding unit consists of one or more directional antennas, some signal processing equipment and an indicator. The antennas and the signal processor determine the bearing of the received signal from the airplane while the indicator displays that bearing with respect to some reference direction, often the heading of the aircraft.

The need of a DF unit to have a directional antenna frequently means that EW receiver has two types of antennas: non-directional ones for search and directional antennas for direction finding. Further, for complete data collection the receiving system should be able to distinguish between horizontal polarization and vertical polarization. This means that an EW receiver must have a minimum of three antennas for each portion of the frequency spectrum. The current trend to combine all these functions into one antenna array does not change this basic requirement.

As we discussed in Chapter 2, an antenna exhibits a preferential direction for receiving energy. A highly directional antenna will collect maximum energy from one direction and exclude most of the energy from all other directions. One method of expressing the directivity of an antenna is in terms of beam width, the width of the main lobe of the antenna pattern. This width is customarily measured between the half-power points of the mainlobe, the points at which the radiated energy has decreased to one-half the maximum as illustrated in Figure 89.

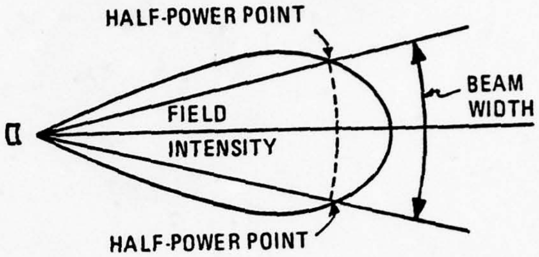


FIGURE 89. AN ANTENNA RADIATION PATTERN

Suppose this highly directional antenna is rotated rapidly in azimuth and the signals received are displayed as strobes extending out from the center of a CRT, with the strobe angular position corresponding to the antenna azimuth. If we mark the display with angular position corresponding to the nose of the aircraft, we obtain a presentation similar to that of Figure 90, where the angular position of the strobe is the same as the angular position of the DF directional antenna relative to the nose of the aircraft, and the length of the strobe is proportional to the strength of the received signal. The result is a picture of the DF antenna pattern pointing in the direction of the received signal. For example, in Figure 90a, the index shows that the signal is from a transmitter at a 60° bearing relative to the heading of the aircraft. In Figure 90b the signal is at 180° bearing relative to the heading of the aircraft.

To determine polarization we might switch between a horizontally polarized rotating antenna and a vertically polarized rotating antenna. The ground transmitter can be assumed to be of the same polarization as the antenna which provides the stronger and more symmetrical pattern on the indicator.

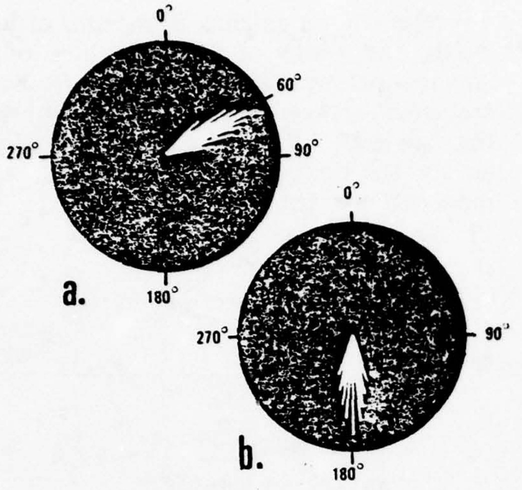


FIGURE 90. TYPICAL DF UNIT INDICATORS

Figure 91 is a block diagram of a typical direction finder unit. The video output from the receiver is introduced into both the beam modulator and video resolver stages. The beam modulator serves as an amplifier and rectifier and emits only positive outputs for any input signal. The positive output signal is applied to the control grid of the CRT causing the electron beam to be turned on when a signal is present.

A simple form of a video resolver is an electromechanical transducer with three windings often called a selsyn or synchro. The movable primary winding is called a rotor and two stationary secondary windings are called stators. The rotor is either mechanically geared to rotate in synchronism with the antenna or electrically coupled to the rotating antenna by use of a servo system should mechanical coupling prove to be inconvenient.

When the rotor of the resolver is in a position to cause maximum induction into the vertical stator and no induction into the horizontal stator an upward vertical deflection is obtained on the scope, indicating that the antenna is intercepting a signal while facing the direction of flight. As the rotor turns the induction into the stators changes, causing the deflection on the CRT to rotate in synchronism with the antenna. Furthermore the total amount of sweep deflection depends upon the signal strength received through the antenna so that a pattern similar to that of Figure 90 is produced on the DF unit indicator.

By now it should be obvious that the DF unit only provides a bearing to the transmitter, the range to the transmitter is not given. To find the transmitter position, called a DF fix, several bearings must be taken at different geographical positions and the

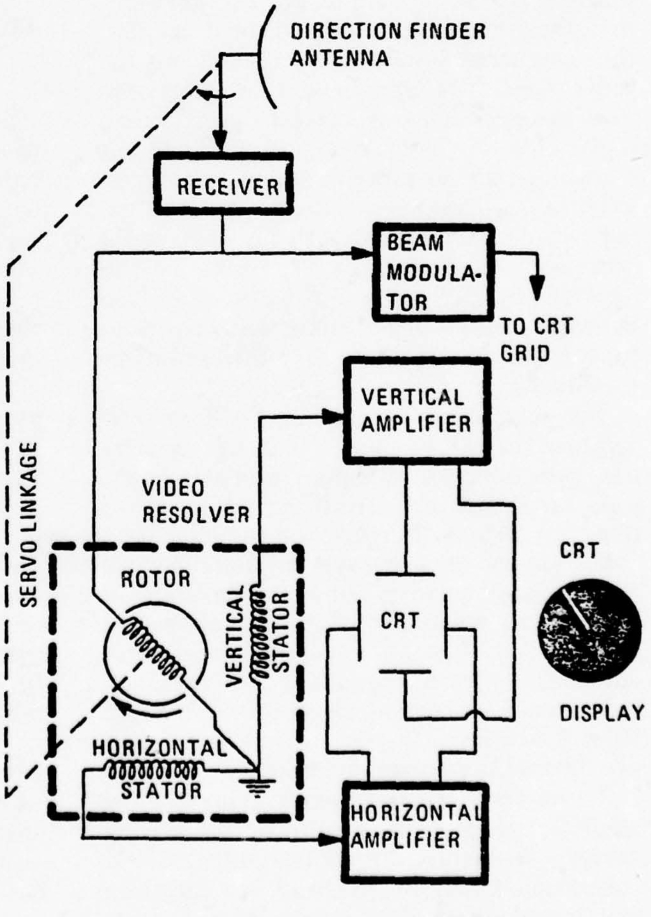


FIGURE 91. A BASIC DF UNIT

bearing determined by triangulation. Because of the limited time in the air, such triangulation is usually done on the ground following the mission unless an airborne computer is available for this purpose.

Basic to the problem of locating a DF fix is the conversion of relative bearings (RB) to the true bearings (TB), bearings with respect to true north. The basic formula is

$$TB = TH + RB \tag{21}$$

where TH is the true heading, the heading of the aircraft with respect to true north. The true bearings can then be plotted on an aeronautical chart to obtain the fix. For example, in Figure 92 the operator adds TH, 025°, to each relative bearing, producing the correct true bearings, 070° and 160°. The true bearings are then plotted from the aircraft's actual position at the time the relative bearings were measured and their intersection is the location of the transmitter. If it were necessary to display a DF fix while airborne a computer could be programmed to collect this data, compute the fix and print out the coordinates of the fix. Such a computer could produce an approximate fix shortly after the minimum angular bearing swing (e.g. 6 degrees) is observed, and then refine the fix (reduce its probable error) as more data is collected.

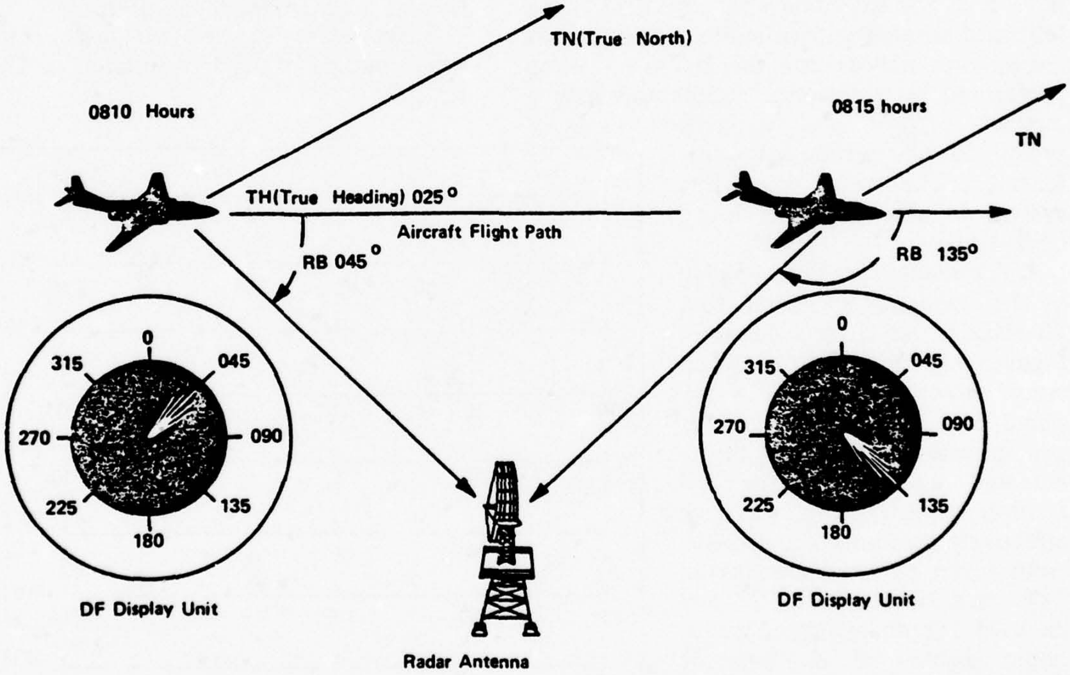


FIGURE 92. THE CONVERSION OF RELATIVE BEARING INFORMATION

Recorders. Normally, EW recorders are audio or video tape recorders that record the audio and/or video signals from one or more EW receivers. However, the term recorder is often extended to include more than just magnetic tape units. Thus, photographs of CRT displays, computer printouts, magnetic tape records of digital data, core memory, and the like should be considered as recorders. Most of these items use the same principles as do the items on the commercial market and will not be discussed further here.

Combined Displays. We have described each one of the various displays separately, but often these displays are combined, for the basic engineering compromises that are made to meet mission requirements often involve satisfying the following two requirements.

1. Be able to display a large frequency spectrum continually so that any threat or signal of interest can be seen instantly. For example, the display may have to cover the frequency spectrum from 30 MHz to 50 GHz.

2. Be able to quickly expand the spectrum or waveform of any single signal for a more detailed analysis.

These two requirements can be met by various combinations of computer controlled and receiver controlled displays. One of the more common solutions is the use of a CRT, a billboard display and an audio warning, with automatic analysis for the billboard being performed by electronic circuits and with a manual control and override system to back up the automatic features. The heart of such a system is often the combined CRT display.

One possible combined display of the frequency spectrum from 20 MHz to 50 GHz is shown in Figure 93. The bottom seven traces show the spectrum of any signal that has sufficient power and proper polarization to be detected by the antenna and receiver system. Thus we have effectively combined the displays from seven panoramic adapters. The trace labeled "FREQ" can be used for an expanded panoramic display of a signal of interest for further automatic and/or manual analysis. The top two traces constitute a pulse analyzer. In this manner, the top three traces in Figure 93 may serve as a back-up for both a recorder and a small digital computer or filter system that does the automatic analysis for the billboard and audio displays.

The Operator-Display Interface

The previous discussion has been almost exclusively concerned with the electronic principles used in a receiver to acquire, process, and display information to the operator. Unfortunately, it often appears that the designer has completed his task when he has arranged a suitable presentation on a scope, a billboard, or a meter. This may well be true if the display is on the ground and the operator is performing detailed analysis of the data. However, if the operator is airborne, then the designer must consider the total environment of the operator in designing a suitable display. Otherwise he may discover that his carefully designed display is essentially useless. So it seems appropriate to conclude our discussion of receiving systems with a look at the man-machine interface.

There seem to be two basic principles which impact on display suitability. The first is:

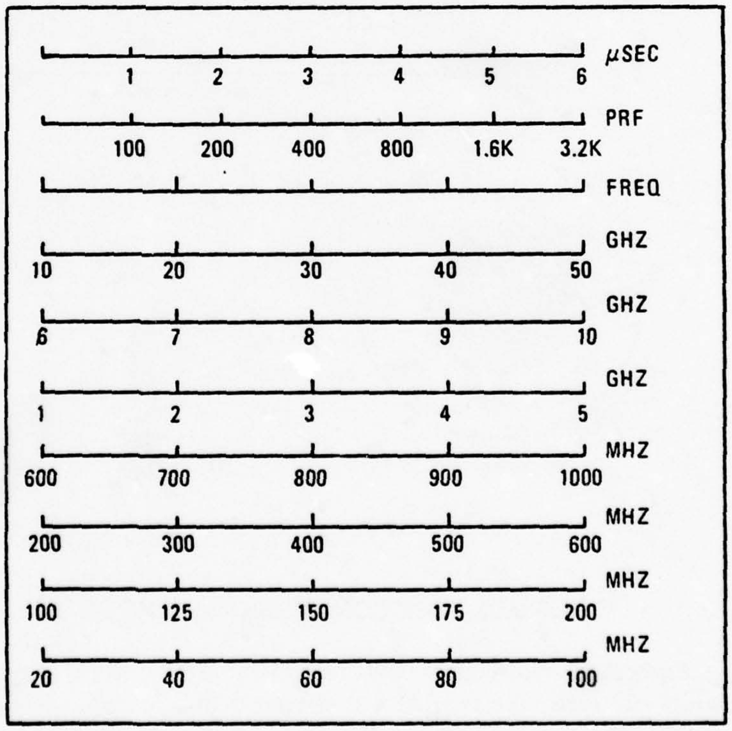


FIGURE 93. COMBINED DISPLAY USING A TEN-GUN CATHODE RAY TUBE

1. *The better the operator-display interface the smaller his reaction time*. In a combat situation survival is clearly enhanced by an ability to assess the situation quickly and react appropriately, for example, start an evasive maneuver to avoid a SAM. Hence we might ask of any operator when viewing a display: After seeing the display do you know what to do? Those displays which present the highest priority information in a manner which leaves no question as to the preferred response are to be desired.

2. *The job of the operator (his crew position) determines both the information he needs and the form or priority of presentation*. It should be obvious that different crew members have different needs for information. A pilot of a single seat aircraft who is engaged in dive bombing is much less interested in detailed threat information than a defensive systems operator of a six-man bomber. Thus we must either provide these two aircrew members with different equipment or we must be able to modify the displays to suit the requirements of the operator.

In addition to two principles the suitability of a display depends initially on the operator's background and crew position. If, in fact, all operators had the same background, this would never be a problem. But there are situations such as in the F-4, where either a pilot or a navigator may occupy a crew position using EW displays (the back seat). After a suitable training period one would expect that such a crew member would develop the same responses no matter what his background. But suppose a new piece of equipment developed through QRC is introduced into a combat aircraft. Because of the QRC development, aircrew training will be minimal and proficiency must be developed through OJT in combat. Now operator background could be very important in determining whether the displays are suitable.

A further consideration of this subject leads us to a third principle.

3. *The suitability of the display depends on:*

a. *The amount and type of information displayed.*

b. *The physical location of the controls.*

The second part of this principle is obvious yet easily overlooked. Again QRC equipment provides a good example. The rapidity of its development will probably preclude a good human engineering of the controls and displays; rather they may be put into the cockpit or crew station, wherever there is room. Thus it is easy to have good equipment which is difficult to operate because of ill-placed controls.

The first portion of this principle in essence says that the amount of low priority information presented must be contingent on the operators other responsibilities and on the threat density of the environment. One may sketch the general relationship as in Figure 94. As the number of threats increases, or as the crew members total job responsibilities increase, then the amount of information presented on each signal should decrease. For example, our dive-bombing pilot is interested only in information on threats which would absolutely prevent him from completing his bomb run. After the bomb is released then he can turn his attention to other matters.

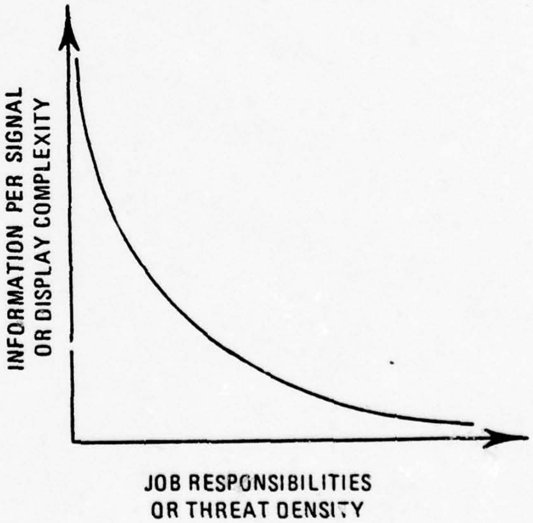


FIGURE 94. DISPLAY REQUIREMENTS

What is the penalty for neglecting these principles? Basically it is a dramatic decrease in effectiveness of the equipment. This decrease usually arises because the operator is presented with much more information than he can absorb. If the operator is saturated with information then his job efficiency will decrease and his total performance will suffer. On the other hand, the operator may take measures to keep himself from being saturated; i.e., he may ignore or turn off the display. In this case the equipment becomes so much useless baggage which could have been left behind.

Thus it is important to realize that there is much more to electronic warfare receiving systems and their displays than the technical design. Once the feasibility of the electronic processing has been established we must still consider the optimum presentation of the information to the operator in order to obtain the maximum effectiveness of the system.

29

AIR DEFENSE SYSTEMS

Since the invention of gunpowder, the gun has replaced the bow and arrow as the principle means of attacking flying objects and creatures. Now surface-to-air missiles and interceptors appear to be replacing the gun as the principle means of attacking aircraft flying at higher altitudes. The current state-of-the-art for the best in-depth air defense system is a balanced combination of all of these weapons systems. Let us look at a modern air defense system with the objective of understanding its composition, the advantages and limitations of its components, how the components are combined, and the response of the system to ECM.

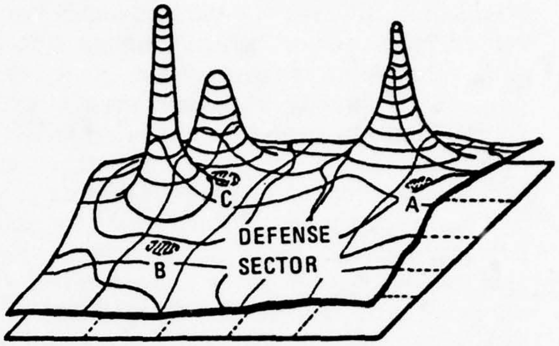


FIGURE 95. PENETRATION DIFFICULTY CONTOURS

The Purpose of Air Defense Systems

The purpose of an air defense system is to prevent penetrating aircraft from destroying their assigned targets. The entire spectrum of defenses ideally blend together to raise the price of penetration to some unacceptable level for a variety of possible threats. Depending on the scenario, unacceptable levels may be only a few percent in the case of repeating tactical air strikes, or possibly 30 or even 50 percent in the case of one-time strategic attacks. From an overall point of view, it is useful to state this goal of air defense in economic terms. For example, given a budget limitation and an agreed upon threat, what would be the best deployment of defenses to insure the survival of Washington, DC, New York City or the continental United States?

A helpful way of visualizing a defense posture is to consider a contour of penetration difficulty as represented in Figure 95. Clearly penetrating target system "A" would be easier than penetrating target system "B", but more difficult than system "C". It should also be fairly obvious that penetrators will seek to optimize destruction and at the same time to minimize risks. Therefore, every resource considered valuable by the defense must have some protective cover—a protective cover roughly proportional to its worth. Or to put it another way, undefended resources, be they wheat fields, lakes, cities or military installations will most certainly be destroyed in the first stages of hostilities.

In order to meet the objective of air defense, a variety of classical strategies are available to the planner. A perimeter defense of missiles or aircraft, for example, could be used; or, a series of point defenses surrounding important, targets might be appropriate. On the other hand, a broad-based area defense, say barrage balloons or hand-held surface-to-air missiles such as REDEYE could cover all possible penetration routes. The number of possible combinations of these individual systems is nearly infinite. The central task facing the defense planner, therefore, is how to integrate his options to insure the maximum survivability over a wide variety of scenarios within the constraint of a limited budget. And all of this must be done with great uncertainty regarding the probability-of-kills expected from each portion of the defense systems.

Tradeoffs between Air Defense Strategies. Let us for a moment examine the defense system in close proximity to a valuable resource, say a major industrial site, strategic military installation or a densely populated urban area. Such a system, most typically referred to as a point defense, consists mainly of AAA or SAM batteries. And, it is common to find point defense systems surrounding Washington, DC, major command-and-control centers, Moscow or ballistic missile launch sites. The point defense system serves the purpose of directly attacking aircraft with gravity bombs who penetrate the near vicinity of a target system. Of greater importance has been the development of overall area defense systems made up of airborne interceptors and large-yield surface-to-air missile systems. The area defense system serves to force attrition upon airborne penetrators which makes the terminal defense problem somewhat easier to cope with, as well as to prevent the wanton destruction of marginally important areas of the countryside.

To explain this important fact, we need to examine the progress of technology in recent years. The development of stand-off weapons has markedly changed the classical defense split between point and area defense systems. With the increasing sophistication and effectiveness of point defense systems, airborne penetrators have sought to avoid penetrating terminal defenses by employing weapons which will permit their launch well outside the lethal range of the point defense. Examples of these weapons are BULLPUP, WALLEYE, CONDOR and SCAD.

If the penetrators can indeed destroy a target system from a standoff lauch position, a new defense scheme working into the extended area around the point defense systems naturally evolves. The result is that greatly increased emphasis must be placed upon the role of airborne interceptors, large-warhead area defense weapons and the relatively inexpensive but highly flexible REDEYE type weapons. Additionally, systematically positioned SAMs, which can be easily moved about, can be deployed to permit a broad smear of defenses well away from the target system, yet still in a position to confront the carriers of stand-off weapons. Most significant in this development is the rapidly assembled, and easily transportable surface-to-air missile presently found scattered over both the United States and Soviet air defense sectors. The mobile SAM provides the air defense forces with the ability to surprise the attack force. Traditionally the military advantage of surprise has been with the attackers, and the shift of the advantage is most significant.

The Mechanism of Air Defense Protection. Because much of our recent experience in air defense has been with Strategic Air Defense, we tend to forget that there are two mechanisms of air defense protection, repulsion and attrition. Repulsion implies that the defense is impenetrable, "leak-proof", that no attacking aircraft survive to reach their targets. In a strategic attack with nuclear weapons repulsion is the goal because only a few weapons can produce unacceptable damage levels. Unfortunately, we have been convinced that such a goal is unattainable and we tend to conclude that all air defense is of little value.

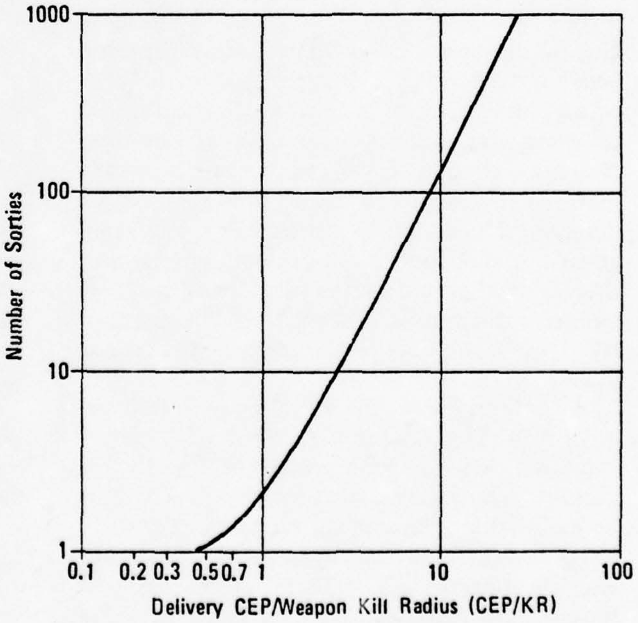


FIGURE 96. THE EFFECT OF DELIVERY ACCURACY ON SORTIE COUNT

What we forget is that in a tactical campaign with conventional weapons attrition is a very potent concept. This arises from one primary factor, the very limited damage radius of conventional munitions, as compared with their typical delivery accuracies. Thus the probability that a ground target will be successfully damaged by one bomb is small, so that many bombs–and many sorties–must be flown. Each sortie which penetrates the defense is an opportunity to "whittle away" at the attacking force, hence a good (but not leak-proof) defense can force such an high cost on the attacker for each facility destroyed that the attacking force is effectively repelled.

In order to see this effect one needs only to consider Figures 96 and 97. The first shows the number of weapons needed to destroy a target as a function of the ratio between the weapon lethal radius and its delivery accuracy. This curve, constructed for a circular "cookie cutter" model, indicates the strong interdependence of these three factors.

The second curve shows the cost of attrition in terms of either force half-life or force replacement time[1] under very simplistic conditions (one sortie per aircraft per day). These curves show that attrition rates of 5 percent are unacceptable for long campaigns, and that rates as high as 1 percent are undesirable. Finally if we use these figures to compute a curve comparing attrition per sortie to attrition per target destroyed as a function of the ratio of lethal radius to delivery accuracy (Figure 98) it becomes very clear that tactical air defense does not have to have a large percentage of success to be quite effective. This is especially true if the ground target is far behind the front lines so that attacking aircraft are exposed to the defense for great distances or long times.

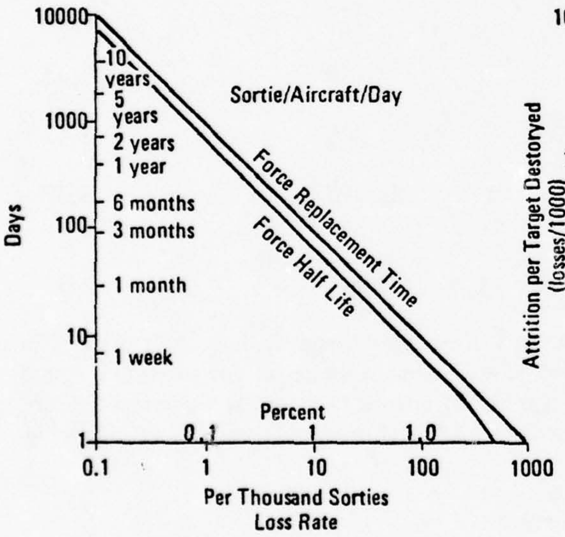


FIGURE 97. THE EFFECTS OF ATTRITION

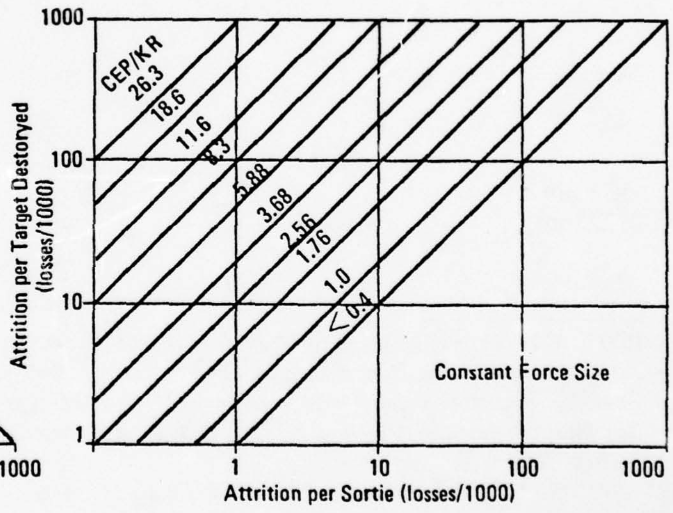


FIGURE 98. EFFECTIVE ATTRITION DUE TO DELIVERY CEP

[1] Force half-life is the time in which the attacker loses one-half his force, assuming he does not replace destroyed aircraft. Force replacement time is the period of time over which the attacker has to replace his original force, assuming he maintains a constant force level.

As an aside it must be noted that this discussion is a very strong justification for the families of "smart" weapons which are coming into the inventory. The purpose of the weapon "smarts" is to increase delivery accuracy through terminal guidance, and the result can be to give the attacker a definite advantage. Consequently, relatively expensive "smart" weapons become cheap when the total cost of destroying a ground target is considered.

Antiaircraft Artillery

The classic role of antiaircraft artillery (AAA)[2] is in point defense. It is found around high value targets, in strategic locations along a variety of penetration routes and around vulnerable points in lines of communication. For example, AAA is often emplaced overlooking the throats of mountain passes that must be used as ground supply routes.

Advantages. When compared to an interceptor or surface-to-air missile system, an AAA piece (a gun) is much cheaper to build and maintain. Consequently, effective artillery pieces become an attractive option to the budget-limited defense planner. In addition, the majority of the personnel operating AAA do not need extensive technical training nor high skill levels. As a result, it takes much less time and money to train a combat-ready artilleryman than it does an equivalent combat-ready pilot, aircrew member, or missile system operator. Maintaining the combat readiness of the artilleryman is also

Table 39

AAA Effectiveness

Weapon	Number of Probable Kills[1]	Rounds per Kill	P_K[2] (%)
90mm	262	225	6.74
40mm	379	239	9.75
37mm	133	286	3.42
.50 caliber (12.7mm)	129	21,897	3.32
Total	903	—	23.3

NOTE: G.M. Barnes, *Weapons of World War II* (New York: D. Van Nostrand Company, Inc, 1947), p 158. This data covers the period from 6 June 1944 to 1 January 1945 in the European theater of operations (1st Army) when 3,888 enemy aircraft were engaged in 1,701 raids. It is also of interest to note that Vakin and Shustov, *Osnovy Radioprotivodystivya*, p xi, state that 500-600 rounds of AAA were required for each aircraft kill in the Second World War.

[1] The observed or estimated number of aircraft destroyed.

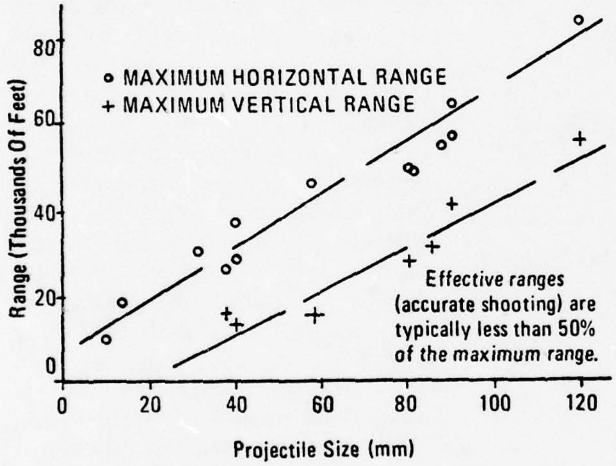
[2] The percentage of the total aircraft engaged that were killed.

[2] The acronym AAA for anti-aircraft artillery stems from World War II when the hyphenated spelling was common. Since that time the hyphen has been dropped but the acronym has remained especially in the Air Force. The Army has changed its acronym to ADA, Air Defense Artillery, and uses this term to refer to both guns and missiles used in an air defense role. We will adopt the acronym AAA both because of common usage and because we want to distinguish between guns and missiles.

less expensive than the equivalent training for the other systems. For example, a small radio-controlled recoverable drone and 45 shells per week cost relatively little when compared to an interceptor that burns $300 of fuel on every flight or a cheap missile which costs $20,000.

The effective methods of employing AAA against airborne targets have been developed over the last 50 years and are well known and not subject to change. Besides keeping the training costs low, this experience reduces the degree of uncertainty as to the success of standard tactics. Data similar to that of Table 39 can be used to estimate the effectiveness of AAA in anticipated tactical situations. Hence, using AAA reduces the uncertainty in the outcome of the battle.

Disadvantages. Yet, in spite of these advantages, interceptors and SAMs have replaced AAA in several important defense areas. This is because there are some serious disadvantages in using AAA.



Effective ranges (accurate shooting) are typically less than 50% of the maximum range.

FIGURE 99. TYPICAL AAA MAXIMUM RANGES

The most severe limitation is the short range of AAA, the weapons used today have approximate effective and maximum range limitations as shown in Figure 99.[3,4] These ranges simply do not meet many of the point defense needs and almost none of the area defense needs against modern strike aircraft.

The next most serious limitation of artillery is the unguided projectile with its long time-of-flight. With muzzle velocities averaging 3000 feet per second[5] medium and high altitude aircraft have tens of seconds to maneuver away from the ballistic trajectory of the projectile with its predetermined point of detonation. Proximity fuses have partially solved the maneuvering aircraft problem, however, their failure rate has been high in combat conditions. A further disadvantage is that in clear weather the muzzle flashes and the stream of rounds (especially if they contain tracers) are visible to the pilot and provide him warning that he is under attack. If the time-of-flight is long enough he may be able to maneuver and avoid being hit. Small bore AAA using tracer ammunition (often termed *groundfire*) is especially easy to avoid.

One means of increasing the probability-of-kill of AAA is to wait until the range is short or the aircraft has passed over AAA site. In the first case the short time-of-flight reduces the maneuver capability of the aircraft. In the second, the pilot's visibility is restricted because the attack comes from his lower rear hemisphere so that his warning is reduced or eliminated. However, this tactic does a poor job of protecting the target under attack by the aircraft and the

[3] The maximum vertical range is approximately 1/2 the maximum horizontal range. This relationship is called Tartaglia's rule by some and can be established from any elementary text in exterior ballistics, for example: Ernest E. Herrmann, *Exterior Ballistics* (Annapolis, Md: US Naval Institute, 1935), pp 12–15.

[4] Data for Figures 99, 100, and 101 is derived from the following sources:
G. M. Barnes, *Weapons of World War II* (New York: D. VanNostrand Co, Inc, 1947).
Will Eisner, *America's Combat Weapons* (New York: Sterling Publishing Co, Inc, 1960).
John Kirk and Robert Young, Jr, *Great Weapons of World War II* (New York: Walker and Co, 1961).
R. T. Pretty, and D. H. R. Archer, *Jane's Weapon Systems, 1969–70* (New York: McGraw-Hill Book Co, 1970).
FM 44-5 (Washington, DC: Headquarters, Department of the Army.)

[5] *Ibid.*

time available for the AAA to shoot at the airplane is reduced.

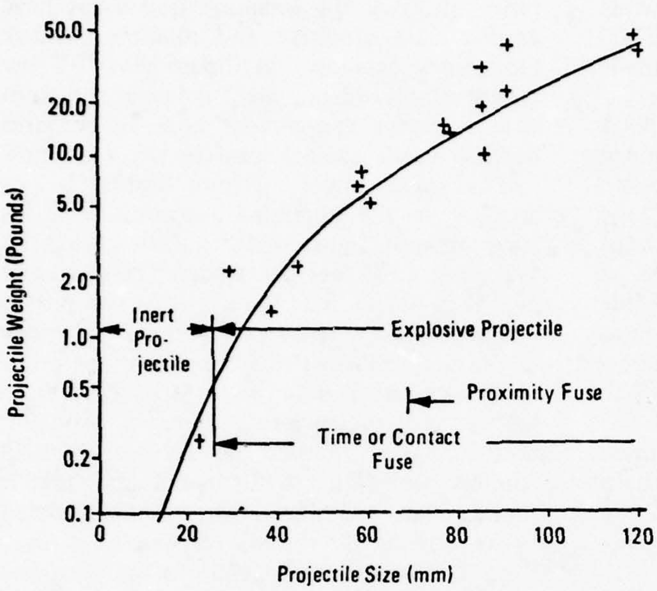


FIGURE 100. TYPICAL AAA PROJECTILE WEIGHTS

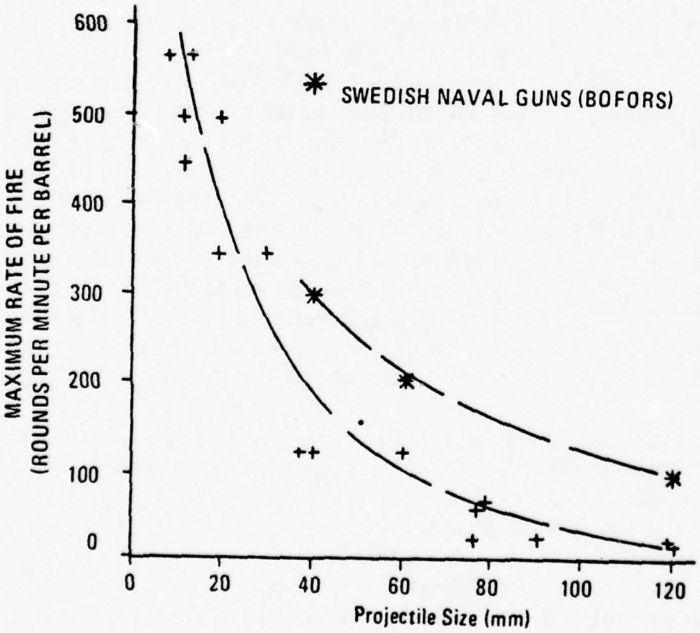


FIGURE 101. TYPICAL AAA RATES OF FIRE

One final disadvantage of AAA is that the destructive radius of the projectile is small, thus the projectile must come very close or impact the aircraft to be effective. Figures 100 and 101 compare the projectile size and rate of fire of typical AAA rounds. Only large rounds with appreciable amount of explosive have lethal radii approaching 50 feet. As a consequence of the small lethal radius AAA either needs accurate target information to make each round effective or it must rely on volume of fire to insure that the aircraft is damaged or destroyed. Thus the larger the caliber of the weapon the more reliance is placed upon determining accurate target position. This effect is illustrated by Table 39 because 50 caliber fire was uncontrolled while the larger weapons were controlled by some automatic aiming system. We will also discuss this effect under AAA tactics.

The data presented in Figure 101 must be interpreted correctly. First the length of time that the maximum firing rate can be sustained depends both on the design of the gun barrel, the method of ammunition feed, and the firing doctrine. If the gun is fired continuously at the maximum rate then the barrel will overheat and have to be changed. The number of rounds that can be fired continuously at the maximum rate is specified for each particular weapon design. The ammunition feed refers to the number of rounds which are clipped together so that they can be fired in sequence. Finally, the firing doctrine specifies the optimum length of burst to meet the previous two constraints and yet achieve best battlefield effectiveness.

AAA Tactics: The basic problem of AAA battery (Figure 102) is to

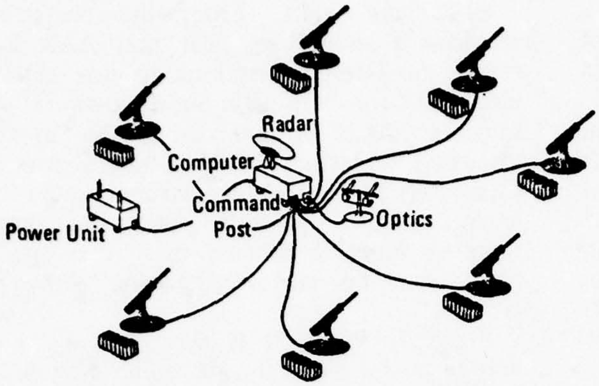


FIGURE 102. A TYPICAL AAA BATTERY

place its unguided, ballistic projectiles near the aircraft. To do so accurately requires a prediction of the aircraft's future position. For large caliber weapons with their slow rate of fire, long range, and consequent long time of flight, *aimed fire* requires accurate aircraft position; so large caliber weapons usually use a fire control system for accurate fire direction. Since radar can give accurate fire even in poor visibility when optical trackers are useless, most modern systems have both optical and radar fire control systems. Generally the radar system is preferred since accurate range measurement is relatively easy with radar, while optical trackers use a stereoscopic range finder which is limited by its short baseline. In either case, gross pointing information (acquisition information) must be provided initially to the fire control system because its field of view is limited.

For smaller caliber weapons the cost of an accurate fire control system is too great to make it worthwhile to provide such a system. As a result these weapons generally rely on visual aiming techniques. If the weapon is small enough so that it can be easily pointed, then tracer ammunition is used and the defense relies on the gunner to solve the prediction problem to make his projectiles hit the aircraft. It sounds like an easy task to make a gun's tracers hit an aircraft, but the problem is complicated by the fact that the gunner is sighting along the line of fire and his depth perception relative to the reading balls of light (the tracers) is very poor. Thus a considerable amount of training is necessary for effective gunnery.[6]

If the weapon is too large for one man to effectively control, another option of the defense is to provide a fire control system, say, for only one out of 10 weapons. This weapon is equipped with tracers and all other weapons are instructed to fire up the tracers of the controlled weapon. In this manner a maximum volume of fire is concentrated in the vicinity of the aircraft.

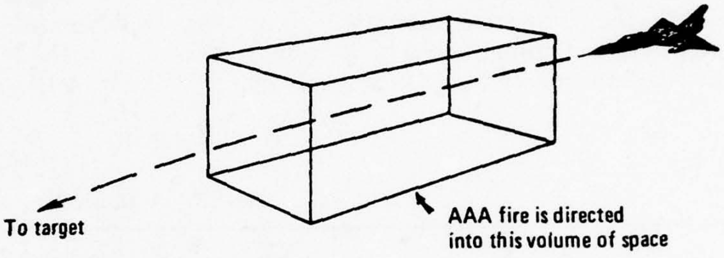


FIGURE 103. THE SHOEBOX CONCEPT OF AAA BARRAGE AND SECTOR FIRE

A further option available to the defense is not to track the aircraft at all. Instead the defense determines the likely track of the aircraft from his expected target, his direction of approach and the terrain. Then the defense puts up a "curtain" of AAA fire such that the aircraft must fly through it. This tactic is called *barrage* or *sector fire* and can be very effective. In essence, the defense fires into a shoebox shaped volume in front of the aircraft (Figure 103). As the aircraft exits the shoebox the fire is shifted into the next shoebox. The shoebox must be large enough, of course, so that the aircraft cannot maneuver around it during the time-of-flight

[6] Robert D. Baldwin, "Tracer Observation for Air Defense Fire Control", *Air Defense Trends* (Fort Bliss, Texas: US Army Air Defense School, September, 1970), pp 65-69.

of the projectiles. This tactic has some psychological advantage in that the pilot can see the bursts from shells exploding in front of him.

Barrage or sector fire is especially useful for point defense since the attacking aircraft must fly a standardized straight-line flight path for several seconds before bomb release.[7] Another use of barrage and sector fire is in the *flak trap*. Here the approaches to an apparently valuable target (it may be a decoy) are lined with AAA sighted in on the expected direction of approach. Many times a flak trap is set up where the terrain provides only one favorable approach to the target. An aircraft ventures into a flak trap to its peril since the restricted approach plus the prepositioned guns result in it running the gauntlet under a very high volume of fire.

ECM and AAA. From the preceding remarks it should be clear that AAA has several well-defined options to use against aircraft. It will help us in our discussion if we tabulate these options using the modes discussed under ECM/ECCM Interaction in Chapter 3. In Table 40 we have separated the angle tracking function from the range tracking function because these two operations can be performed using different systems.

From Table 40 it is clear that ECM is limited in the effect that it can have on AAA fire. Even if the tracking radar is rendered completely ineffective the defense still has a very capable optical tracking system. All that is needed, once the defense has deduced the penetrator's target, is altitude information from the defense radar net. In clear weather

Table 40

AAA System Modes

		Tracking		
Mode	Acquistion	Angle	Range	Fuzing
Automatic	(Radar Net)[1]	Tracking Radar	Tracking Radar	Proximity
Manual	Acquisition Radar[3]	Tracking Radar[2]	Tracking Radar[2]	Proximity/time
Alternate Input	Radar Net	Optical Tracker	Optical Tracker	Time
Backup	Optical Tracker/ Visual[4]	Barrage/Sector Fire	Height-finder Radars[5]	Contact

NOTE: The columns of this table are independent of each other; that is, the acquisition. angle tracking, range tracking and fusing subsystems may be operating in different modes.

[1] Assuming that the radar net has sufficient accuracy and that the data is cross-telled to the AAA site.

[2] Operated in a manual mode.

[3] Typically the AAA acquisition radar is not automated.

[4] The unaided human eye.

[5] Given aircraft altitude and the location of the "shoebox" approximate range is easy to determine.

[7] This statement is true for all known delivery systems for non-terminally guided bombs. A sufficiently sophisticated terminally-guided bomb might allow release from a wide variety of aircraft attitudes; likewise one could conceivably build a sophisticated bomb sight which would compensate for a wide variety of aircraft attitudes upon release of a non-terminally guided bomb. But high accuracy (low CEP) in both these cases may still require standardized flight paths which will quickly become known to the enemy, and thus provide him the opportunity to use barrage or sector fire.

an optical sight is typically more accurate than a radar in azimuth and elevation. The capability for optical tracking becomes even more potent when it is realized that in a tactical situation visual bombing is preferred for delivery of a large quantity of bombs on the target. If the aircraft has to see its bombing then there is a good probability that the defense can see the aircraft, and if precise optical tracking is impossible Table 39 shows that a high volume of fire in a barrage/sector mode can be very effective.

The effect of AAA in the above situation is to enforce a minimum altitude below which an aircraft is reluctant to venture because the high volume of fire and the short range accuracy produce high losses. Consequently, the defense benefits because higher altitudes mean greater inaccuracy in bomb delivery.[8] The reaction of the attack to this defense can take four forms.

1. The attackers may ignore the targets so protected for other targets, thus yielding to the objective of the defense.

2. The attackers may use standoff weapons thus reducing their losses.

3. The attackers may attack the defenses directly in a *roll-back* attack. However, in the aircraft-gun duel the cost exchange ratio[9] is usually favorable to the defense.

4. The attackers may use defense suppression tactics to reduce their losses. In these tactics anti-personnel weapons and bombs are delivered to the vicinity of the operating AAA sites during the time the strike force is on their bomb run. The objective is to make the

Table 41

The Major Functional Components of a SAM System

Component	Function
Acquisition Radar	Provide early warning Determine gross target position and velocity Determine target priority
Target Tracking Radar	Determine precise target position and velocity
Missile Tracking Radar	Determine precise missile position and velocity
Computer	Calculate missile launch, steering, and warhead detonation commands
Missile Launcher	Get missile airborne in the approximate direction of the target
Command Guidance Link	Transmit computer commands to missile
Missile Autopilot	Stabilize the missile Fly the missile as directed by the commands received from the command guidance link
Missile Fuzing	Determine when to explode the warhead
Displays	Provide backup operational capability

[8] Gravity bombs are ballistic weapons also. The greater the release altitude the greater the effect of small position and velocity errors on release, thus the greater the inaccuracy.

[9] The ratio of the cost of the aircraft (if destroyed) to the cost of the AAA weapon (if destroyed).

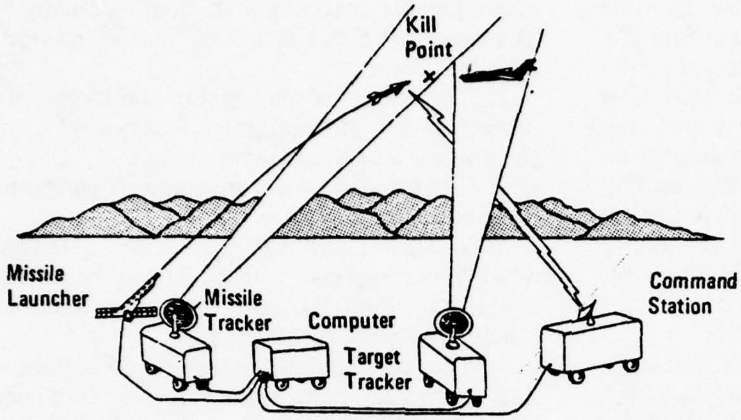


FIGURE 104. A TYPICAL SURFACE-TO-AIR MISSILE SYSTEM

AAA gun crews take cover when the strike aircraft are most vulnerable–during their bomb run. Which of these options is most effective depends upon the tactical situation.

Surface-to-Air Missiles

In an effort to overcome the limitations of AAA, the surface-to-air missile (SAM) has been developed. A large rocket or jet engine and stabilizing wings (fins) have been attached to the projectile (warhead) to greatly extend its ballistic range. Also, a guidance unit and control fins have been installed to give the projectile the ability to (1) intelligently chase a maneuvering target and (2) correct initial firing errors. However, the advent of the SAM has not solved the long time-of-flight problem of AAA.

Advantages and Disadvantages. The SAM is a flexible weapon system that is extremely effective in the proper circumstances. Early planners estimated each SAM fired had a 50 percent chance of downing its target.[10] If the target does not maneuver this figure may be true, however, "friendly airliner" (non-maneuvering) targets are surely the exception rather than the rule in combat. Furthermore, SAM systems use electronic sensors, and the missile emits infrared radiation from its engine during launch and flight, hence, RHAW equipment can give the pilot information about the location of the SAM and how great the threat is.

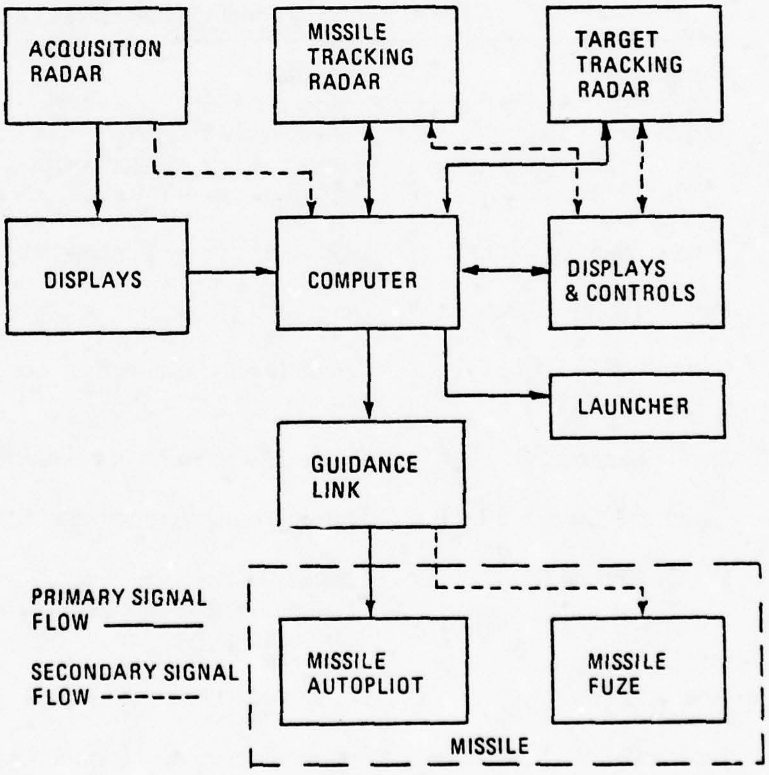


FIGURE 105. A TYPICAL SAM SYSTEM BLOCK DIAGRAM

[10] Vakin and Shustov, *Osnovy Radioprotivodystiviya*, p xi.

The SAM as a "smart" projectile has added a few problems of its own. It is a generally much more costly and complex weapon system,[11] as shown in Table 41 and Figures 104 and 105. A SAM site of six missiles may be manned by an entire army battalion, whereas the AAA site of eight guns may be operated by a platoon or company. The increased complexity requires that at least several of the SAM operators have high skill levels and extensive technical training. Hence, a nation can afford to build and deploy far fewer SAM sites than AAA sites.

In general, SAM systems have three weaknesses. First they tend to be ineffective at very low altitudes (below 1,000 feet) because it is difficult to get good radar coverage at those altitudes, especially at distances from the site greater than several miles. Second, their complexity makes them relatively slow to respond to intruding aircraft compared to AAA systems. And third, each site has a limited number of rounds available for immediate use. However, these weaknesses are complemented very well by AAA systems, with the result that a combination of SAM and AAA systems make a very potent defense.

The very complexity of the SAM system means that a much greater potential exists to degrade its operation with electromagnetic signals. Because the increased range of the SAM makes optics less desirable than radar for range, azimuth and elevation, it is more vulnerable to interference by ECM. Furthermore, in-flight missile guidance tends to relax the requirement for accurate launch parameters so the shoe box in Figure 103 becomes much larger than for AAA and barrage/sector fire is much less attractive. If the guidance data is degraded by ECM the SAM loses the advantages of its ability to correct its flight path to the target. In fact, ECM could potentially be used to send the SAM wrong information and steer it out of harm's way. It is even conceivable, but not too likely, that one might "capture" control of the SAM and steer it toward a target of the penetrator's choice.

SAM System Operation. Before we can discuss how EW can be effectively used against SAM systems we must be familiar with the operation of the SAM system itself. The purpose of the acquisition radar or early detection subsystem (Table 41) is to prepare the SAM system to engage the attacking aircraft. Although the ability to rapidly engage an aircraft depends upon the state of the readiness of the system and its operators, there is a minimum reaction time below which system effectiveness decreases rapidly. Hence, the early detection system will seek any indication of impending attack to alert the missile site. The existence of ECM is *prima facie* evidence of attack and does not degrade this aspect of the system function.

The other aspects of the early detection system function are imposed because the target tracking radar needs fairly accurate aircraft coordinates to insure a responsive and reliable lock-on and track capability. EW can seriously degrade this function and force the SAM system operators to use a less desirable procedure for target acquisition. For example, if the acquisition radar has automatic detection and tracking circuits, these may be disabled or misled by the ECM. In this case the operators may use a manual radar scope as a backup method. If the ECM is still too strong, or they realize they are attempting to find a false target. they may use target information from the area defense net to initially point the tracking radar in the direction of the target. They may also employ the target tracking radar to search in the expected direction of the attack in the hope of finding one of the attackers. But this tactic is usually a last resort since the narrow field of view of most precision radars makes target acquisition in this situation very improbable. In any event. ECM against the acquisition radar can degrade the SAM system effectiveness by disrupting its normal routine so that the reaction time is increased.

The brain of the system is the computer. It has as inputs the target position information

[11] This discussion does not consider the very short range SAM, such as REDEYE, which is more properly considered as a man-portable, large-caliber AAA weapon of short range.

from the target tracking radar and, after the missile is in flight, the missile position information from the missile tracking radar. Its job is to direct the missile to the target aircraft to destroy it. The computer outputs are often launcher pointing commands, launcher firing commands, missile guidance information and commands, and, in some cases, warhead detonating commands. The job of the computer is usually so complex that there is no backup system; however, the computer may have backup algorithms to use if its input data is degraded by ECM.

Both the target and missile tracking radars are customarily designed to operate automatically; however, this mode is usually the most susceptible to active ECM. Thus a provision for manual operation (an operator watching a radar scope) may be provided. A further backup input might be an optical sight to be used to track the target, the missile or both. An alternative scheme could be to put some target homing device in the missile itself. That is, the missile senses radiation from the target and steers toward the target. If the radiation is that of the SAM tracking radar reflected from the target, it is called *semi-active homing*; if the missile contains both the transmitter and receiver, it is called *active homing*: and if the radiation is from the target's jamming transmitters it is called *home-on-jam*. Here, the computer functions have been divided between the ground site and the missile itself.

A SAMs flight is often described as three distinct guidance phases. They are (1) launch or initial course guidance, (2) midcourse guidance, and (3) final or terminal guidance. A SAM may be designed to use only one type of guidance (like infrared) for its entire path or it may be designed to use several guidance schemes. For example, a SAM may use a combined pre-programmed inertial guidance procedure from launch until after booster separation. Then command guidance is used to steer the missile to within 5 miles of a target. The missile's own active homing system may then lock on to the target and complete the terminal guidance phase.

Each type of guidance has its own vulnerability to ECM. And each type of guidance can have several variations. For example, the command guidance link can take one of several forms. It may be a separate radio link with its own transmitter and receiver or the pulses of the target tracking radar may be coded to transmit steering command to the missile. A third option is the beam-rider system in which the missile seeks the center of the target-tracking radar beam. Since the missile receiver antenna is pointed away from the intruder and toward the ground transmitter (the best possible geometry for ECM protection) there is rarely a backup for the ground-to-missile command guidance link.

The final function of fuzing customarily takes one of four forms: proximity, contact, time, or command fuzing. A proximity fuze is a small independent radar set in the missile itself that detonates the warhead when the missile is close to the target. ECM against a proximity fuze must be done well, it must explode the warhead at a great distance from the target, or it may actually aid the fuze in accomplishing its purpose. Command fuzing uses the computer determined relative position between aircraft and missile to tell the missile when to detonate. It can be affected by anything which affects the computer input data. Time and contact are purely mechanical methods of fuzing which are independent of the rest of the system after launch.

From this discussion it is clear that there may be a tremendous range of variability between missile systems and ECM may have different effects depending upon the options available to the missile system operators. In addition, SAM system performance is also constrained by its design (for example, missile aerodynamic limitations), mechanical jitter and target maneuvers. System design also affects the missile path, for the optimum path may not be the shortest path to the target. Some missiles ascend vertically to their operating altitude, and then after completion of the boost phase they are commanded to turn toward the target intercept point. Other missiles may take the shortest path to the target in order to reach the target in minimum time. The geometry of the missile path is only limited by the capabilities of the system (missile maneuverability, range, speed, or operating altitude requirements, and the computer program).

SAM and ECM. Properly interfering with any of these functions will degrade the system operation and thus is favorable to the attacking aircraft. However, the SAM operator in a properly designed system has several methods of accomplishing each function and he may well choose a less effective alternative when confronted with ECM in order to retain some capability or in order to achieve surprise. Such alternative courses of action, as listed in Table 42, will limit the maximum effectiveness of any particular ECM technique and must be considered in EW planning.

Table 42

SAM System Modes

		Tracking			
Mode	Acquisition	Target	Missile	Guidance	Fuzing
Automatic	Radar Net[1]	Tracking Radar	Tracking Radar	Radio Command[2] Beam-Riding Semi-active Homing Home-on-Jam Active-homing	Proximity Command[2]
Manual	Acquisition Radar[3]	Tracking Radar[4]	Tracking Radar[4]	Radio Command[4]	Command[4]
Alternate Input	Radar Net Tracking Radar	Optical Tracker	Optical Tracker	————[5]	Time
Backup	Visual	Barrage Fire	————	Ballistic Trajectory	Contact

[1] Assuming that aircraft position data is automatically cross-telled to the SAM site.

[2] Automatic operation under computer control.

[3] Assuming that the acquisition radar is manually operated.

[4] Manual operation of the equipment (computer disengaged).

[5] In the presence of ECM home-on-jam would be a reasonable backup to any of the other guidance systems.

Properly used EW can reduce the SAM to an even lower level of effectiveness than the AAA discussed previously. The only alternative left can be barrage fire of SAMs into a shoebox so large it will take hundreds of $10,000 to $20,000 SAMs to effectively fill the box shown in Figure 103. On the other hand their size and complexity makes SAM sites more vulnerable to attack by aircraft than AAA sites. The need for a large amount of radar information also makes them especially vulnerable to anti-radiation missiles or glide bombs. Thus SAM sites become suitable targets for hunter-killer or defense suppression operations by the penetrators, especially since their fewer numbers give a better opportunity for a few aircraft in such a role to be successful.

Area Defense

In contrast to the previous two systems which are usually localized, the area defense system encompasses the total defended area. As such it will include AAA and SAM systems, but it also has its own long-range weapons. Traditionally the weapon of the area defense system has been the manned interceptor and the system itself has been called the EW/GCI radar net. But with the advent of the long range SAM, such as BOMARC, the distinction on the basis that the area defense weapons are manned is fading. A better distinction seems to be on the basis of weapon control. If the control of the weapon can be passed from one site to another then the system is an area defense; if control cannot be so shared then the system is a large point defense. On this basis the SPRINT anti-ballistic missile becomes a point defense and only such weapons as the manned interceptor and BOMARC become area weapons. We shall adopt the convention of calling point missile defenses SAM defenses and the area defenses the EW/GCI defense.

Manned Interceptor. The primary weapon of the area defense is still the manned interceptor. Of the three destructive weapons discussed in this appendix, the manned interceptor can be the most effective; it is also the most expensive weapon to build and maintain. The interceptor is very mobile—it can fly to new bases of operation quickly as the defense situation changes. If properly designed, it can operate from grass fields or roads. The interceptor's range is limited only by pilot endurance since the amount of fuel it can carry can be supplemented by air-to-air refueling. The aircraft is also inherently very flexible. It can be a part of a tightly operated ground-control-intercept (GCI) system, or it can operate independently. Its engagement time is limited only by its weapon payload and pilot endurance since it can remain in a holding pattern with a tanker for hours and make repeated intercepts until its weapons are expended.

There are two divergent trends in the design of interceptors. First is the traditional short range, light, small. very maneuverable, uncomplicated interceptor that can perform well in a dog-fight. This aircraft may or may not use extensive GCI since it is designed for close-in visual attack. The second trend is toward large, sophisticated, long range, very high speed (over Mach 3) interceptors that hit and run under close GCI control. This philosophy is to intercept the attacker at great distances from the target area. Then defenders have time to reattack the surviving penetrators several times. It appears that a good defense-in-depth would have both types of interceptors.

Table 43

Estimated Defense System Cost Ratios

	AAA Gun	AAA Battery	SAM Missile	SAM Battery	Interceptor	EW/GCI Net
AAA Gun	1					
AAA Battery	10	1				
SAM Missile	10	1	1			
SAM Battery	100	10	10	1		
Interceptor[1]	200	20	20	2	1	
EW/GCI Net	20,000	2000	2000	200	100	1

NOTE: These are minimum estimated ratios of the cost of the item on the left to the item heading the column.

[1] The cost of pilot acquisition and training for manned interceptors is omitted.

The advantages of the interceptor are gained at a considerable cost. First, the aircraft must be based and maintained. Even if it can be operated from unprepared fields, the defense must provide maintenance facilities, equipment and personnel and some sort of control facilities, as well as quarters for the crew members (pilots and radar operators). The skill levels of all the personnel involved are also required to be higher because the weapon system is more complicated and sophisticated. This impacts both on the training requirements and on the quality of the facilities that must be provided.

We can illustrate this increase in complexity by comparing the acquisition cost of the interceptor with the other two systems as in Table 43. Considering the fact that an F-4 interceptor costs in the neighborhood of 2–3 million dollars, area defense systems are very expensive indeed. The costs cited are only acquisition costs, the maintenance costs and personnel costs could be expected to be no less than 1/10 the acquisition costs per year.

In general, the interceptor itself is not the final weapon for destroying the penetrator, it is only a mobile launching platform for the weapons that make the final kill. Typically, its weapons consist of guns used for close-in visual attacks and missiles used for standoff, radar or infrared controlled attacks. Thus the interceptor has the modes of operation in an ECM environment shown in Table 44.

EW/GCI Nets. In order to control and guide the expensive interceptor, a defense needs an extensive radar and command and control net. Typically this net embodies both early warning (EW) and ground-controlled intercept (GCI) functions. The combination of the EW/GCI radar net and the interceptors can be considered as an area defense system which has the major functions listed in Table 45. It must be realized that this system really has two parts. The ground portion exists to position the interceptor so that it can make an attack on the penetrating aircraft. Once in position, the interceptor acquires the target itself and proceeds to guide itself or its weapons against the penetrator. Thus, in contrast to the AAA or SAM systems, the area defense makes no attempt to use ground systems to provide terminal guidance for its weapons.

Early warning for the area defense is usually provided by radar, although many overt and covert methods have been used in the past. These methods include both active

Table 44

Interceptor System Modes

Mode	AI Search and Track	AAM Guidance	AAM Fuzing
Automatic	Automatic	Automatic	Proximity
Manual	Range only & optical[2]	————[1]	————[1]
Alternate Input	Ground Control[4]	Home-on-Jam	Contact
Backup	Visual[3]	Optical[3]	———

[1] Typically no manual capability is provided.

[2] An optical sight with the radar providing range.

[3] A gun sight.

[4] In some cases ground control may be the preferred method, especially with automatic data link capability.

Table 45

Area Defense. Electronic Subsystems

Subsystem	Function
Early Warning (EW) Radar Net	Detect penetrating aircraft Alert the defense Determine track and size of the raid
Ground Controlled Intercept (GCI) Radar	Monitor the position of all friendly and enemy aircraft Direct the interceptors to a position favorable for an attack on hostile aircraft
Identification-Friend-or-Foe (IFF) Systems	Identify friendly aircraft
Height-Finder (HF) Radar	Determine the altitude of hostile aircraft Maintain track on hostile aircraft
Computer	Determine intercept point Perform data storage and retrieval for ground controllers and ground commander Provide information for displays Direct interceptors
Filter Center	Display the air battle situation Control the air battle as the commander directs
Ground-to-Air and Air-to-Ground Communications Link	Pass instructions and replies between the ground controller and the interceptor
Airborne Intercept Radar	Acquire the penetrator Steer the interceptor to weapon/missile release point
Air-to-Air Missile (AAM) Guidance	Guide the missile to the target
AAM Fusing	Detonate the missile in proximity to the target

and passive (radiating and non-radiating) techniques such as ground observation posts. electronic receivers (passive detection), reports from ships and airliners, etc. All these reports are submitted to a centralized command center. the *filter center*, which evaluates them, issues the appropriate warnings to the civilian population, and places the various military units in the proper alert status. At that point the control of the air battle usually passes to the GCI system.

The GCI system attempts to keep track of all elements of the air battle using its radars and communications links. Its job is to provide the commander with an up-to-date picture of the air battle so that he can effectively deploy the fighters and engage the point defenses, and to carry out his orders as he directs weapon commitment. The operation of the GCI system is controlled from the filter center, where the air situation is displayed to the defense commander. Because of the complexity of modern air defense, modern air defense systems have employed computer systems to solve their data processing problems. Using computers, however, is no panacea; as the complexity of the system increases one senses that the software debugging problems should increase as the square of the complexity. Consequently, we find both automated and manual defense systems in use throughout the world and we shall examine both in more detail.

Manual EW/GCI Systems. The primary job of the air defense commander is to allocate his forces to prevent the penetrators from damaging his nation's resources. To do so he uses the system diagrammed in Figure 106. Since he is charged with a large geographical area to defend, he must use several radars to keep that area under surveillance. Typically the information is fed from the several radars surveying the area into the filter center where an up-to-date picture is maintained of the position of all friendly and hostile forces. In a manual system this picture is maintained by plotting the positions manually on a large board containing a map of the defended region. From the apparent track of the penetrators in relation to their likely targets and the defenses the commander designates the weapons to engage the attackers. These designations are usually mutually exclusive between interceptors and point defenses, that is point defenses and interceptors do not usually engage the penetrators simultaneously because of the likelihood that the interceptors will be shot down. Once the decision has been made to commit weapons, then the necessary acquisition information is passed to them and the filter center assumes a monitor role.

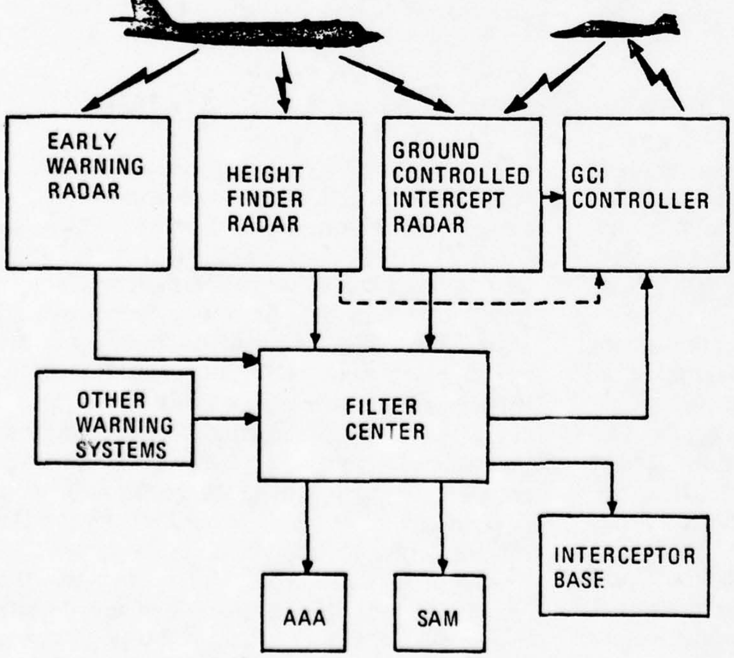


FIGURE 106. A MANUAL EW/GCI SYSTEM

If the weapon is an interceptor then the interceptor must be scrambled by notifying the fighter base and the proper controller assigned. Interceptor control is usually assumed by a weapons controller located at the radar site covering the area in which the intercept is to take place. The controller plots successive positions of the penetrator and the inteceptor on his PPI scope with a grease pencil. From these plots he can determine speed and track and thus determine the most favorable position for the interceptor to acquire the target and complete the intercept.

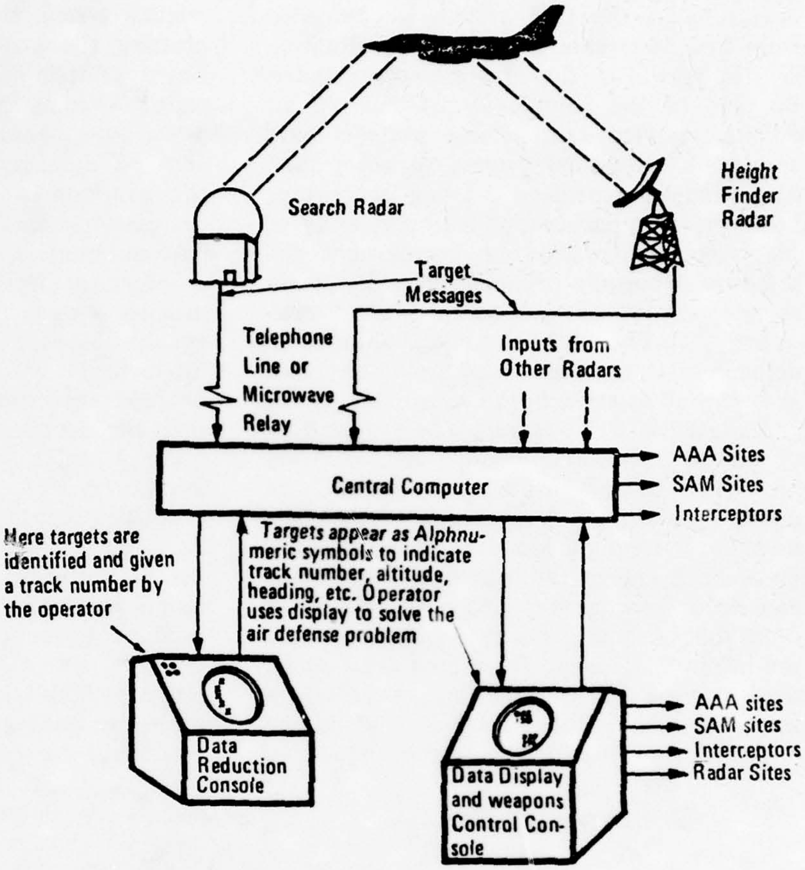
During this process the defense must obtain the altitude of the penetrator. Thus a height-finder radar is commanded to turn to an appropriate azimuth and locate the penetrator. From his scope the height-finder operator is able to read the penetrator altitude. In addition, if the height-finder is co-located with GCI radar, then it may be used to complete the intercept if the search radar is usable to paint the penetrator due to a malfunction or because of ECM.

If the penetrator should pass out of the controller's view because of delays in the interceptor's arrival, the filter center will assign the intercept to another controller.

From this description it is clear that the manual EW/GCI system is very redundant. Its chief limitation is that all the operations necessary to keep track of the air battle must be done by hand. With the advent of high speed aircraft the time delays in this essential accounting function have become so great as to reduce the effectiveness of the system to unacceptable levels. Hence most modern systems employ digital computers.

Computerized EW/GCI Systems. Automating the EW/GCI system with computers can take place in three stages.

1. The filter center can be automated.
2. The interceptor control function can be automated.
3. The target detection and tracking function can be automated.



Search Radar
Height Finder Radar
Target Messages
Telephone Line or Microwave Relay
Inputs from Other Radars
Central Computer
AAA Sites
SAM Sites
Interceptors
Here targets are identified and given a track number by the operator
Targets appear as Alphnumeric symbols to indicate track number, altitude, heading, etc. Operator uses display to solve the air defense problem
Data Reduction Console
Data Display and weapons Control Console
AAA sites
SAM sites
Interceptors
Radar Sites

FIGURE 107. A COMPUTERIZED EW/GCI SYSTEM

In all three stages the rapid computation and data retrieval capability of the computer is used to assist the human operator or commander. Typically, the decisions are made by men.

Automating the filter center uses principally the data storage and retrieval capability of the computer and associated transmission facilities. The computer stores the information about the hostile aircraft and all the information pertaining to the status of the defense–weapon position and readiness, weather, weapon characteristics, etc. Upon command, this information can be presented on displays to assist the commander in determining his defensive strategy and in allocating his weapons.

If the interceptor control function is automated then the computer is used both to store information of interest to the controller–such as recovery airfield status–and also to calculate various parameters (such as time to intercept). If the system is well automated, the detailed guidance of the interceptor may be done automatically through a ground-to-air data link.

Automating the target detection function involves designing a system which will recognize when the radar returns have a pattern characteristic of an aircraft. When the returns indicate an aircraft, its range and bearing is calculated and sent to the remainder of the system by appropriate messages. Typically automatic target detection requires a large track capacity because all returns meeting the detection criteria become tracks whether they be important, unimportant or spurious (clutter, ECM). A target is detected by assigning a track number to it. If the target tracking function is automated then the computer will examine subsequent radar returns, select the one that represents the new postion of the aircraft, and update its internal files with that new position.

In our own SAGE system all three areas have been automated. Figure 107 illustrates the general form of the system.[12] Because of the automation the system has several distinguishing characteristics. First, since the target detection function is automated at the radar, all target positions are represented in numerical form in the remainder of the system. Thus, when displays of target position are made on a weapon controller's scope, the display is not a PPI scope but a synthetic display reconstructed from the internal computer files. Second, because all information is stored in computer updated files the operators have access to factual information from the computer which the manual operator must keep himself. In many cases this information can be presented on the operator's scope in alpha-numerical form in juxtaposition with the symbol representing the aircraft position. Third, since information comes into the computer from many different radar sites, the system can choose or ignore data from certain radars depending upon its quality or usefulness to the combat situation. Last, the system is quite centralized since all the functions except target detection are performed at the central computer.

ECM and Area Defense. From the previous discussion, it is clear that an area defense is both complex and redundant. For that reason the highest priority of ECM is usually against the interceptor and its

Table 46

EW/GCI System Modes

Mode	Early Warning	Aircraft Position	Identification	Communication
Automatic	Automatic strobe detection	Automatic detection and tracking	Automatic IFF	Data Link
Manual	EW Radar operators	GCI Radar operators	Response to commands	Voice
Alternate	GCI radar operators	EW radar	Preplanned maneuvers	Broadcast[1]
Backup	Passive detection Observers	Passive detection (triangulation)	Inspection by interceptors	———

[1] Using other than the usual ground-to-air channels, for example, navigation aids or commercial broadcast stations.

[12] The basic concepts of the SAGE System are described in the following three articles, all published in the *Proceedings of the Joint Computer Conference*, 12, 1958.

R.R. Everett, C.A. Zraket, and H.D. Benington, "SAGE–A Data-Processing System for Air Defense", pp 148-155.

W.A. Ogletree, et.al., "AN/FST-2 Radar Processing Equipment for SAGE", pp 156-160.

P.R. Vance, L.G. Dooley, and C.E. Diss, "Operation of the SAGE Duplex Computer", pp 160-163.

weapons. Then ECM is employed selectively against EW/GCI radar net. Table 46 shows the different potential modes of operation of the ground radar net and underscores the difficulty of degrading the system without attacking all its elements.

Furthermore, ECM and penaids used against the ground radar system affect the radars principally by introducing time delays in the identification of aircraft position and track. In order to affect the filter center or the computerized command and control system, the ECM must either continually deny this position and track information to the system or it must seek to provide so much information that the system is overloaded. The comparative advantage of either of these approaches depends both on the method of converting "raw" radar data to aircraft tracks and on the internal data processing performed on the track data.

Let us return to the interceptor. The use of ECM against interceptors usually is done in a series of steps. First the early warning radars are fed false information so that the position and numbers of penetrators are not known. Thus the defenders do not know how many interceptors to launch, when to launch them, or where to establish the holding pattern. For example, one or two penetrators may feign an attack and make themselves look like a hundred aircraft. If the defenders launch the interceptors and do not have air-to-air refueling capability, then the interceptors will be out of fuel when the real attack arrives.[13]

The second step occurs when the penetrators are within the range of the interceptors. During this phase all penetrator electronic warfare efforts are directed toward preventing an interceptor from finding a penetrator. Conversely, the interceptor will use extensive ECCM to help him find a penetrator.

Next, when a penetrator and interceptor find each other, then the penetrator's efforts are directed against the interceptor by:

1. Breaking the lock-on and confusing the interceptor's precision fire-control radar with ECM.

2. Making the interceptor follow a false target generated through ECM so the penetrator can escape.

3. Locating (visually or through RHAW) and outmaneuvering the interceptor and all weapons he may use.

4. Popping the proximity fuses of any weapons before they reach the penetrator.

5. Destroying the interceptor.

The interceptor's ECCM efforts are directed toward:

1. Destroying the penetrator, or failing that

2. Disrupting the penetrator's plans so badly he cannot complete his mission.

These events can occur at a furious pace and an outcome is usually obtained in a few minutes.

Thus the inherent mobility and flexibility of the manned interceptor is the only air defense system that can match the penetrator on an equal basis. In a sense, any well-trained aircrew is the necessary adaptive, self-programming, specialized computer that controls the engagement to its advantage.

The Structure of Air Defense Systems

The foregoing narrative discussion of ECM and air defense tells very little about what kinds of ECM are effective, and how the system responds to the ECM. To discuss this we must understand the basic structure of an air defense system. That is we must be able to answer the question: What are the causal mechanisms which influence the system behavior under attack? There is very little literature available on this subject but the ideas presented previously provide a basis for our discussion of this question.

Information Processing. Basically an air defense system is an information processing system. It does have physical resources—men, guns, missiles, and aircraft—which it controls, but its control over these resources is dependent upon its processing of information about the threat. So let us first look at the information to be processed.

It is the natural tendency of anyone schooled in the sciences to think of information theory when someone mentions information. The result of this is to start thinking of the information flow in terms of

[13] Price, *Instruments of Darkness*, pp 223-234, gives some good examples of the effectiveness of feints.

bits, channel capacities, entropys, etc. Although such ideas have good theoretical underpinnings, their application to the subject of air defense systems is fraught with so much uncertainty that they become almost useless. For example, what is the channel capacity of a radar set, of a radar operator, of the defense commander? How much information is represented by an aircraft track? As a result it appears that these questions are the wrong questions to ask.

A much more fruitful approach seems to be the management approach called systems dynamics.[14] In this approach information is handled by its outward manifestations, sheets of paper, aircraft tracks, etc. This information is subject to four defects which reduce its value.[15] They are:

Error
Bias
Distortion
Delay

These four defects have differing effects on information processing systems. It can be shown that their effects on a system increase in the order shown. That is, error has the least effect and delay the most. Let us discuss these defects individually and apply them to an air defense system.

1. *Error* is the randomness of information. It is usually conceived as the result of a noise-like signal being superimposed on the true value. In an air defense system error arises naturally because of the noise-like signals in the radar sensors. However, the system is designed to cope with this phenomenon by smoothing or averaging. That is, the perceived values are averaged over a long enough time that the random fluctuations tend to cancel out and the true value remains. Hence the system is resistant to error.

It is unfortunate that one of the basic concepts of ECM is to add noise to the radar signal, that is, to increase the error of the information. We say unfortunate because the built-in smoothing makes the effect of light ECM very small. And even moderate ECM can be handled by increasing the smoothing, i.e. by averaging over a longer time. In fact, ECM only becomes effective when the required averaging time becomes so long that the effect is more of a delay. This is the meaning of Figure 32, jamming only becomes effective when it obscures the target return. Likewise, false target generation is effective only when the averaging time necessary to discriminate the true targets from the false becomes long.

2. *Bias* is the term used to describe a persistent deviation of the perceived situation from the real situation. I.e., if the air defense system always overestimates or underestimates the size of the attacking force then it has bias. It can be shown that the effect of bias depends upon the dynamics of the system. If the perceived raid size is checked with the actual raid size then bias can be removed. Unfortunately, unless one can visually inspect the raid bias may persist. Now one of the purposes of penaids is to introduce bias through decoys, false targets, etc. A feint or false penetration is another source of bias. Finally, the air defense system may have a built-in bias through its intelligence information. The problem of bias points out one of the subsidiary functions of the interceptor, to remove bias through visual observation.[16]

3. Although information *distortion* has many forms, one of its major forms is sampling. Because of the limitations of its sensors, an air defense system only obtains a panoramic view of the complete air situation about once every 10 seconds.[17] Experience has shown that this is adequate to control the air battle. But one of the effects of ECM is to slow down the sampling rate. This slow down occurs either because the ECM conceals the actual aircraft positions so that

[14] As exemplified by Forrester, *Industrial Dynamics* and *Principles of Systems.*

[15] C.V. Swanson, "Evaluating the Quality of Management Information" Sloan School Working Paper No 538-71 (Cambridge, Mass: Massachusetts Institute of Technology, June 1971).

[16] The Germans made use of their aircraft in this role in World War II. See Price, *Instruments of Darkness*, p 162.

[17] Typical scan rates of most long range search radars are 5-10 rpm.

only occasional glimpses of their positions are received, or because the data processing load on the system increases so much that it cannot process all the information in the time between samples, thus it must take fewer samples. In either case the performance of the system begins to deteriorate.

The tactic of the strike force making several turns en route to the target is designed to exploit the effect of sampling. For if the sampling rate does slow down, then the turns will cause a large divergence—distortion—between the actual air situation and the situation as seen by the defense.

4. *Delay,* the last information defect, is usually the most serious. It is a general, theoretically-established characteristic of all dynamic feedback systems that their performance deteriorates as their internal delay increases. The next section will show that an air defense system is a feedback information processing system, hence delay will degrade the system performance. ECM can cause excessive delay by several means. We have already mentioned that increasing error can cause delay through increased smoothing times. Furthermore, a decreasing sampling rate might be considered as an increased information delay.

But there is also another mechanism, that of psychological pressure created by the threat of attack and the uncertainties that accompany it. This mechanism has two effects. One is that the alerted defense system responds much faster than the unalerted one. Thus the function of the early warning network is to alert the system so that its internal delays are reduced. Hence, it is the objective of the attacking force to give as little warning as possible—in a word—to surprise the enemy.

The other effect is that the commander will often delay a decision because his information is uncertain. The propensity for a commander to so act is obviously a very variable human quality but the pressure is still there, and the resultant delay might have serious consequences.[18]

In summary, it appears to be much more fruitful to discuss the information handling capacity of an air defense system in terms of the possible information defects rather than in terms of information theory.

Basic System Structure. We mentioned previously that the basic information structure of an air-defense system is that of a feedback loop. This aspect is often overlooked in many descriptions. Often we think that we have said all that needs to be said about air defense when we have described its components as we did earlier in the chapter. But that view overlooks the interconnections of these components. More important, that view does not explain why the system behaves as it does. For example, only looking at an air defense system as a feedback information processing system explains why early warning and system delays are important. Yet any military commander can tell you from experience that warning and delay are two supremely important parameters.

We will not try to justify the feedback structure we are about to propose. Rather, once it is stated it becomes almost self-evident. But this structure is so important that it should be considered the basic causal structure of the system because it is the basis of the system behavior. Hence we can call Figure 108 the air defense causal diagram.

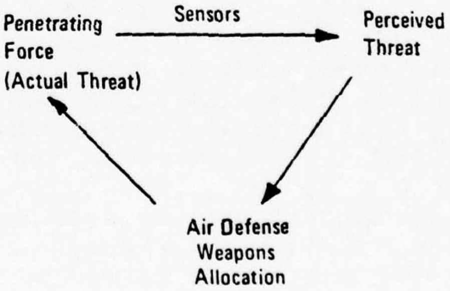

Penetrating Force (Actual Threat)
Sensors
Perceived Threat
Air Defense Weapons Allocation

FIGURE 108. TYPICAL AIR DEFENSE ORGANIZATION

[18] There are many examples of this tendancy. The actions of Commander Bucher of the Pueblo is one.

Although the closed loop structure of Figure 108 is appealing it needs to be refined to be useful. But the refinement should keep the emphasis on structure rather than components. On the other hand we should be able to identify the major units of an air defense, since major units usually have well defined functions in the structures. Finally, the structure should be able to allow for ECM since ECM is potentially one of the major contributors to information defects in combat.

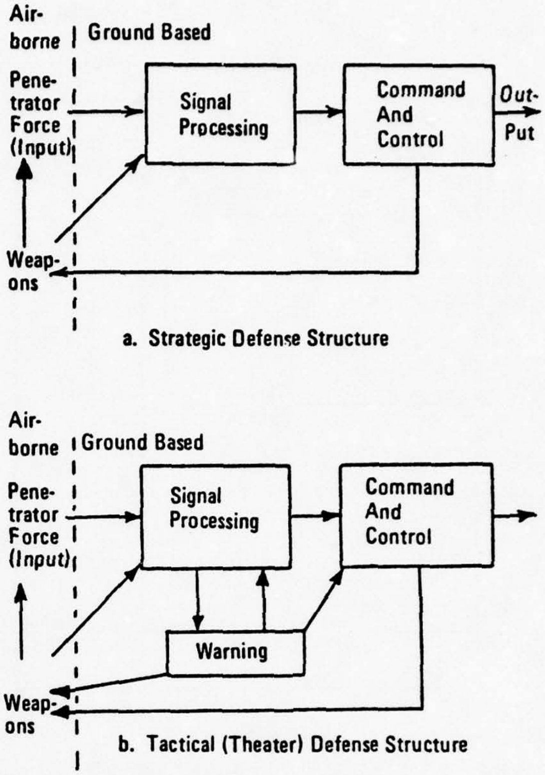
The input to any air defense system is the physical presence of an attacking force, and its response is the physical destruction of penetrators or defense weapons. Unfortunately the response cannot be measured accurately until after the conflict when one can sort out the pieces on the ground. Hence that outcome is difficult to use as a criteria to measure goal seeking success, yet some criteria is necessary to drive the system toward its goal.

The answer to this problem lies in the fact that the greater part of an air defense is an information processing system. This system has three major subsystems:

1. Signal Processing
2. Command and Control
3. Warning

These components in conjunction with the penetrators and the defense weapons form the closed-loop system shown in Figure 109a. The alert reader will be quick to note that warning is not included in that structure. The reason for this omission is that the only function of warning is to decrease the system response time; once that has happened warning ceases its function and the system becomes that of Figure 109a. In strategic air defense the usual assumption is that the system is fully alerted, so that warning does not affect the system response.

On the other hand a tactical air defense system, such as a theater air defense, is much more subject to surprise attack. Under such conditions. the air defense system must begin operation in a transient mode in which warning plays a vital part (Figure 109b).



a. Strategic Defense Structure

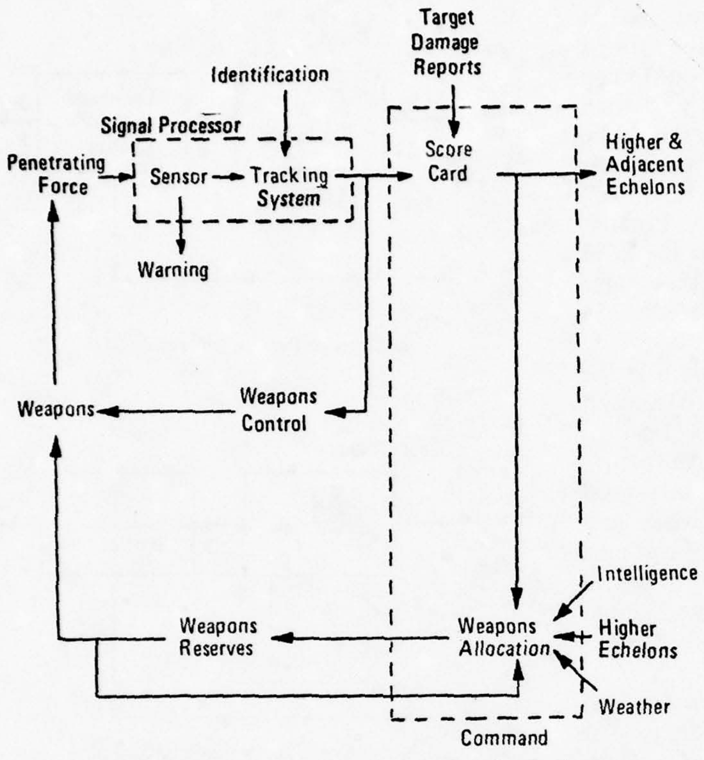
b. Tactical (Theater) Defense Structure

FIGURE 109. BASIC AIR DEFENSE STRUCTURES

Figure 109 shows that typically most of the information processing is done on the ground. The connection between the air vehicles and the ground is typically electromagnetic radiation of some kind. It is at this point where ECM enters the structure, since it can be added to the signals from ground-to-air or from air-to-ground. It should also be observed that the signal processing subsystem has to process signals from both attackers and defenders.

In order to identify this structure more closely with typical air defense functions Figure 110 expands Figure 109. In this figure we have excluded the warning subsystem outputs for simplicity. The output of the system is called a "score card". This is a "how-goes-it" function which the defense keeps as a record of its accomplishment. and is the sensible output of the system in battle.

From these figures it is clear that most of the information used by the command and



Note: Warning Subsystem Outputs Have Been Deleted For Clarity

FIGURE 110. A TYPICAL AIR DEFENSE SYSTEM

control functions comes from the signal processing system. Hence it is here that the information defects should be first observed. It appears worthwhile to examine this subsystem in more detail before we look at command and control.

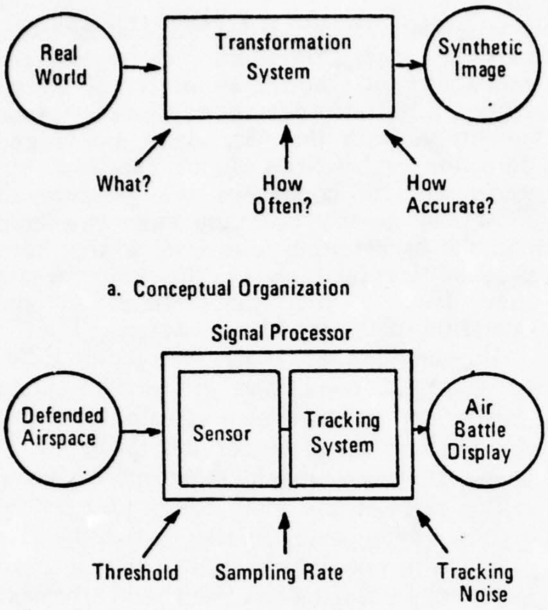
Signal Processing Subsystem. From our previous discussion the signal processor can be defined as that part of the air defense system which takes the electromagnetic signals in the atmosphere and converts them into data useful for the command and control subsystem. Although common technical usage would tend to place the signal processor after the sensor (the radar) in actual fact the sensor may do signal processing both in receiving the radiated signals which are its inputs and in transmitting signals also (e.g. a pulse-compression radar). Hence we will consider the signal processor to include the sensors and all other equipment in the information processing chain up to the command and control subsystems.

The major question which has yet to be answered is what is the output of the signal processor. Although one might vary the placement of the boundary without affecting the basic structure of the system, one logical placement follows from the realization that the function of the air defense system is to operate on the physical positions of relatively remote air vehicles. Hence the first need of the system is accurate position and velocity data on all these vehicles. Thus we shall take the output of the signal processor to be the estimated position and velocity data on all objects under surveillance, that is, an air battle display.

Now the signal processor can be considered as an electronic camera which attempts to reconstruct a synthetic image of the real world. As such there are three questions we need to know to evaluate its performance. First, what are the classes of objects which are included in this synthetic image? Second, how often is the image renewed? And third, how accurately does the image correspond to the real world? This model can be diagrammed as in Figure 111a. Figure 111b re-labels this diagram to correspond with the typical parameters of an air defense system.[19]

The class of objects included in the synthetic image is determined by the radar threshold. A high radar threshold implies that only returns from sizeable objects are accepted by the system, while a low threshold

[19] Some of this analysis was suggested by R.A. Flink, "An Investigation to Determine If An Industrial Dynamics Type Model Can Contribute to the Design and Development of an Air Traffic Control System", (Master's Thesis, MIT, Cambridge, Mass, June 1966).



a. Conceptual Organization

b. A Typical Realization

FIGURE 111. THE SIGNAL PROCESSING SUBSYSTEM

means that returns from small objects are accepted. Physically, the radar threshold is represented by the AGC (automatic gain control) voltages in the radar receivers and the switches that determine their ECM configuration.

The specification of how often the signal processor takes a picture of the real world can be stated as the system sampling rate. For example, if the radar system is automated and feeds a computer then the sampling rate is the rate at which the computer surveys the complete air situation and updates the air battle display. But if the radar system is a manual system, then the sampling rate is the average rate at which the operators survey the air space. This average is not the usual concept of the average over all standard trained operators but the average over all operators who may have the airspace under their surveillance, and includes the effect of their varying work loads. Since a radar operator is an adaptive signal processor and may vary his scan depending on the tactical situation presented him, there is no readily available physical measure of this quantity in a manual system. Nevertheless, the considerations discussed previously under information errors leads us to believe that the sampling rate is an important parameter of the radar system.

The question of the accuracy of the synthetic image can be discussed by specifying both the mean and standard deviation of synthetic image position errors and the percentage correctly labeled as friendly or enemy. Such an approach implies that the errors can be modeled by a gaussian noise (tracking noise) added to the real positions as detected (according to the radar threshold) and sampled. The mean and standard deviation of this noise are controlled by the signal processor itself. The labeling process, often called identification, is composed of two parts. One part uses flight plan information and the observed positions to establish the correct label. The other uses a supplementary radar beacon (IFF/SIF, sometimes called *secondary radar*) to establish the label. Both these processes are degraded by ECM, but in different ways, since the former relies on tracking accuracy while the latter does not.[20] In combat the second method is likely to be the more common. Hence, tracking noise could be modeled as a monotonic function of ECM and relative target position.

Given that the major output of the signal processor is a synthetic image of the air battle one of the key issues in air defense is the accuracy of this image. If the image is accurate, then the commander and the weapons controller have essentially perfect and complete information with which to allocate and direct their weapons. In this case the defense planner has been successful. If the synthetic image is incomplete then the offensive planner has been successful.

[20] Clearly if the tracking is inaccurate there may be insufficient correlation between aircraft position and predicted flight-plan position for identification. Even more disastrously, there may be good correlation between hostile aircraft and friendly or neutral flight plans with inaccurate tracking.

Since the air battle display is a vital part of the air defense system it is natural to expect that the information defects in the system are manifested principally as errors in vehicle positions in this synthetic image. The objective of low level penetration with its low data rate and low sampling rate is to create significant errors in this image. Likewise, the objective of ECM, false targets, and decoys, with their high data rates and potential for system saturation, is also to create significant errors in this display. Hence an important measure of effectiveness for the air defense system itself is the *track association* percentage. The track association percentage is the percent of the time that the vehicle position of the synthetic display is both within a certain distance (is associated with) the real vehicle position, and is correctly identified.

It must be understood that track association is not a useful quantity in combat since its measurement requires cooperative penetrators. But in training and evaluation exercises flying safety dictates that penetrator positions be monitored by someone, usually a "trusted agent" or umpire. Thus, accurate data is available to determine this effectiveness measure.

Conversely, the effectiveness of ECM and penetration tactics could also be measured by track association. One advantage of this measure of effectiveness is that it is a direct, factually-based measure. This is in contrast to such measures as penetrators killed, defenders killed, or targets destroyed, which in non-combat of necessity involve a simulation of the lethal mechanisms.

ECM and Signal Processing. Before leaving the subject of the signal processor, let us consider more deeply the effect of ECM on the radar threshold, sampling rate, tracking noise and identification. Of these the radar threshold may have the most far reaching effects. The radar threshold is usually determined by the average signal-to-noise level in the radar receiver. It is typically set high enough so that the maximum radar returns can be easily distinguished from the inevitable background noise. As the threshold is raised the noise is more and more rejected, thus the probability of mistaking noise for an object in the airspace, a false alarm, is reduced. On the other hand, raising the threshold increases the probability of ignoring an object in the air space, a missed detection. Under normal conditions both the false alarm and missed detection probabilities can be kept low, but under combat conditions the presence of ECM can modify both the radar threshold and the background noise level so that both probabilities increase to the point where they have a significant effect on the operation of the air defense system.

The sampling rate is also affected by ECM. In non-ECM conditions the sampling rate usually increases to some nominal value set by the physical scan rate of the radars themselves. However, under conditions of heavy traffic or ECM, the computation load on the system may become so heavy that all the data available in one radar sweep of the air space may not be able to be processed before the next radar sweep. At this time, the system and its operators have a choice, either complete the computation before starting over or decrease the computation load. Both choices potentially involve throwing away good data, and the desirability of either approach depends on its ultimate effect on the air defense performance. The desirability of either choice and the ways that the effects of that choice can be modified would also seem to be important topics in air defense system design and operation,

Finally, tracking noise is also affected by ECM. Now tracking noise is not the same as the noise-like signal sometimes used for ECM. Instead it is a representation of the fact that when the radar does sample a vehicle position, it sometimes obtains the wrong sample value. In non-ECM, good-weather conditions the tracking noise should be small since clutter and other spurious returns can be observed and compensated for. But with ECM the signal processor must choose the most likely position for the vehicle and this will probably be a return near the predicted position at the moment of sampling. Hence ECM could cause a considerable increase in tracking noise.

As we stated previously ECM affects the identification process in two ways. If identification is made by comparing the flight plan position with actual position, then the major

3

effect of ECM will be to make identification uncertain because aircraft position is uncertain. One might suspect, however, that the total uncertainty in identification will be greater than the position uncertainty because of the psychological impact of ECM. That is, since the total air picture is uncertain all identification is suspect.

Identification by flight plan, however, will not be the predominant approach in combat since flight plans (or fragmentary orders, "frags") can change at the last moment. Thus a more direct identification feature is desired, such as is provided by radar beacons, or IFF/SIF. If identification is provided by radar beacons then their radiation is susceptible to ECM, both jamming and deception. In this case the ECM affects only the identification process. But if these beacons are also used for tracking, and this is a very tempting approach since the beacon signal is usually stronger than the radar return and often on a different frequency, then ECM against the identification affects both identification and tracking. In this case the tracking noise for friendly aircraft is likely to be different than for enemy aircraft while the identification accuracy will be some function of ECM type (jamming or deception) and strength. Whether gaussian noise is a good model for these effects is not readily apparent.

Although these four parameters have been discussed separately, their effect on the track association percentage is not additive. Identification, tracking noise and sampling rate all depend in some manner upon the radar thresholds in both primary and secondary radar channels. In the primary radar channel a low threshold will not only increase the apparent data rate and thus tend to lower the sampling rate, but the increased data rate implies that the tracking noise will also increase. Likewise slow sampling rates will tend to multiply the errors due to tracking noise to the detriment of track association. Hence the control of radar threshold and sampling rate are very important to successful theater air defense.

In the secondary radar channel the signals are usually well above the noise, hence ECM will have only minor effect on the sampling rate. Rather it will directly contribute uncertainty to tracking and identification by suppressing the signals by increasing the threshold.

Command and Control. The basic function of the command and control is to manage the air battle. This management proceeds at two levels. One level is the command function which addresses the overall direction of the air battle. The other one is the control function which directs the weapons so that their effectiveness is maximized.

Basic to effective management of the air battle is some appreciation of the overall defense effectiveness, some sort of "score card". This is the basic information that the commander uses, in conjunction with the threat information provided by the signal processing subsystem, to direct the battle and to inform his superiors of the progress he is making.

The commander's direction of the battle is essentially that of deciding which of his resources to use against the penetrators. As input data he has the estimated position, velocity and identification of the penetrators, an assessment of the probable target, a knowledge of the strengths and weaknesses of the defense, directives from higher headquarters and the the score card relating past success. The objective of the commander is to neutralize the penetrators with minimum expenditure of his resources and minimum target damage. He has a dynamic programming problem in which the relationships are likely to be nonlinear and time-varying. For this reason, the commander's function is rarely automated. However, this weapons allocation function completes the major closed loop in the defense system, hence its characterization probably has a major effect on the defense system response.

The very fact that the judgement involved in weapons allocation is not automated suggests that it is the least well understood element in the air defense system. It is very likely, however, that every commander has developed a set of operating rules, rules of thumb, or policies which he uses to guide his decisions and style of operation. These policies in fact determine the response of the weapons allocation process to its inputs, and may be critical in determining the overall system response.

The above discussion does not mean to imply that no study has been made of weapons allocation; in fact, many have been made and most contribute to the commander's insight of air battle management. But it appears in retrospect that the larger part of these studies have considered weapons allocation as an open-loop process. That is, the threat and its uncertainties affect the allocation which in turn affects the battle outcome (under uncertainty also), *but the allocation in itself never affects the threat or its uncertainties.* Hence, the dynamics of the system must either come from the threat or be assigned by *fiat* to the system itself. It is the author's contention that placing the weapons allocation process within a feedback loop should help us to see what effect command policies have on the system response. For example, dispatching aircraft to observe the penetrators would close a loop around the signal processor to increase track association and thus make later weapons allocations more effective.[21]

In this light, the effect of information defects on the performance of the system should be a very revealing study. For the closed loop formulation should reveal how resistant the air defense of the assumed structure is to each defect. Likewise it would be of great interest to know which strategies and which structures are least affected by the information defects.

The other major portion of the command and control, weapons control, concerns itself with directing the weapons assigned by the command function to the most favorable engagement geometry. The inner loop of which it is a part seeks to minimize the weapon-penetrator distance under the constraints of the permissible weapon engagement geometries. Its control over the weapon exists in the form of steering commands transmitted to the weapon (desired headings and velocities of interceptors, steering commands to surface-to-air missiles, or elevation and azimuth angles of AAA gun barrels). The return signals which measure weapon response come through the signal processing system even though there may be direct two-way communication with the weapon. For there is enough potential randomness and sluggishness in the weapon response that the weapons controller typically relies on sensor data to verify that his commands are being carried out. Hence, we can expect the dynamics of this inner loop to have a significant impact on the management of the battle by the commander.

Warning. The warning susbystem has the task of alerting the remainder of the system that a threat exists and thus reducing the response time of the remainder of the system. The inputs to the warning system are two in nature. One is detection of unanticipated aircraft in the air space, the other is detection of hostile acts, such as the presence of ECM. The physical variable that approximately reflects the response time of the system is the alert condition. This is termed an approximate correspondence because the alert condition is usually designed to designate the steady state response time after the initial transient has passed. In so far as the geometry of the confrontation gives the defense alert condition time to respond, this is a good characterization; however, in short intense conflicts the transient state may be important. Hence, one benefit of this approach might be a better elucidation of the conditions under which warning is important.

System Response. How does an air defense system respond to a penetrating force? It is difficult to answer this question because much of the information is classified. Furthermore it is common to describe the system in terms of summary statistics rather than dynamically. However, we can draw a general diagram of what we might expect to see.

To do so we use a portrayal similar to that used to describe the effect of ECM on an air defense system in Chapter 5 (Figure 48). But

[21] See Price, *Instruments of Darkness*, p 162, for an illustration of this policy.

in this case we make the abcissa the percent defense area denied and we plot curves of constant percent MA (mission accomplishment). The result is Figure 112.

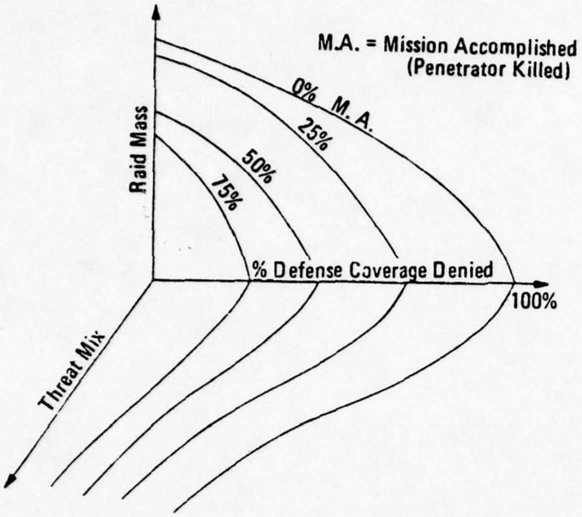

M.A. = Mission Accomplished (Penetrator Killed)
Raid Mass
0% M.A.
25%
50%
75%
% Defense Coverage Denied
100%
Threat Mix

FIGURE 112. AIR DEFENSE SYSTEM PERFORMANCE

The defense area denied is that portion of the raid area as defined in Chapter 5 in which the air defense system is unable to maintain tracking on an aircraft. Unless triangulation is used, it is roughly all the raid area which is outside the burnthrough range of the radars. The percent mission accomplishment is the success ratio of the defense, the percent of weapons engaged (AAA firing, SAM salvos, or interceptors) which result in destruction of a penetrating aircraft.

Unlike previous ECM descriptions this figure adapts very well to low altitude penetration. In that case the loss of defense coverage is due to terrain masking of the aircraft as well as to ECM. If the raid is all at low altitude, we must decide how to compute the raid area. In this case it may make sense to compute the raid area using the single coverage altitude rather than the actual raid altitude. The single coverage altitude is the minimum altitude at which the defense radars can track aircraft at any point within its political borders.[22]

[22] We mean over ground area within its political or military control. This restriction is only necessary for small nations. it would be meaningless over the interior of the US.

APPENDIX D

DETECTION AND LOCATION OF AIRCRAFT BY RADIO METHODS

Sir Robert Watson-Watt[1]

1. It appears unsafe to base any method for the detection or location of enemy aircraft on any of the primary radiations from the craft. Lamps and radio senders will not be used on a scale permitting detection. Sound from engine propeller and structure is steadily being reduced, and is in any case subject to extreme vagaries in propagation which, while still permitting detection, may prevent location. Electromagnetic radiation from ignition sytems is readily screened to very low values. Infrared radiation from engine is so heavily and variably absorbed in a water-laden atmopshere as to make it an unreliable indicator.

2. Of the secondary radiations, excited by "illuminating" the craft by ground installations emitting light, heat, sound or radio-waves, the first two are excluded by atmospheric absorption (especially in cloudy conditions). The use of sound waves above the audible limit has some attractions, but the low power rating of emitters and the low velocity of propagation–a small multiple of the speed of the craft–are against it. It appears, in sum, that the only moderately promising method of detection and location is that of secondary "wireless" radiation.

3. The most attractive scheme is that of setting up zones of short-wave radio "illumination" through which the approaching craft must fly. The most desirable form of the scheme will be discussed in more detail.

4. Let it be assumed that the typical night bomber is a metal-winged craft, well bonded throughout, with a span of the order of 25 meters. The wing structure is, to a first approximation, a linear oscillator with a fundamental wave length of 50 meters and a low ohmic resistance. Suppose a ground emitting station be set up with a simple horizontal half-wave linear oscillator perpendicular to the line of approach of the craft and 18 meters above ground. Then a craft flying at a height of 6 kilometers and 6-kilometer horizontal distance would be acted on by a resultant field of about 14 millivolts per meter, which would produce in the wing an oscillatory current of about 1½ milliamperes, per ampere in sending aerial. The reradiated or "reflected" field returned to the vicinity of the sending aerial would be about 20 microvolts per meter per ampere in sending aerial.

5. It is at present common practice to put 15 amperes into the sending aerial, giving a received field, from the reradiating craft, of the order of a tenth of a millivolt per meter after generous allowance for losses. This value can in effect be more than doubled in the pulse technique without overload in the transmitter. If, further, the method proved so reliable that general "illumination" could be abandoned and a thick sheet of "illumination" at a convenient inclination could be relied on, this field could be increased at least tenfold by the provision of a suitable beam array, of practicable dimensions and cost, at the ground station. It will be observed that this last improvement is obtained at some sacrifice of easy watch, as an indication is obtained only while the craft is "illuminated", in the one case the illumination is weak floodlighting of a very large area, in the other it is strong searchlight illumination in an inclined sheet of small thickness.

6. It is not wholly fantastic to suggest that the span of the machine could be measured, to aid identification, by a rapid sweep of the emitted radio frequency, but

[1] Sir Robert Watson-Watt, *The Pulse of Radar: The Autobiography of Sir Robert Watson-Watt* (New York: The Dial Press, 1959), pp 427-434. This is the famous "Death Ray Memo" of 1932.

without emphasis on this possibility it will be noted that the simpler scheme will lose in efficiency as the emitted frequency fails to fit the resonant frequency of the wing structure. The resonance curve of the wing and fuselage structures will be very flat; this militates against easy span measurement but in favor of easy distance measurement; without change of radio frequency to fit the craft, a variation of two or three to one in span will not much affect sensitivity. This also reduces sensitivity to changes in aspect of the craft as in strong cross winds. On balance, however, it may be concluded that reflected fields of the order of a millivolt per meter are readily attainable at 10 kilometers rising, by the use of an alternative height of aerial, to the order of 10 millivolts per meter as the craft passes overhead at heights under 20,000 feet. These fields are about 10,000 times the minimum required for commerical radio communication, so that very large factors of safety indeed are in hand for ranges of the order of 10 miles at flying heights of about 20,000 ft.

7. If now the sender emits its energy in very brief pulses, equally spaced in time, as in the present technique of echo-sounding of the ionosphere, the distance between craft and sender may be measured directly by observation on a cathode-ray oscillograph directly calibrated with a linear distance scale, the whole technique already being worked out for ionospheric work at Radio Research Station. In the examples already taken the reflected ray would return after 50 microseconds for 6 kilometers horizontal distance and after 40 microseconds from overhead. I believe these times to be quite manageable within the technique, though they involve a very considerable shortening of the pulse durations now used (about 200 microsec), or an artifice, which we can certainly provide, for reading the time of return even when the reflected pulse is superposed on the primary timing pulse which has arrived at the receiver by a very short ground path. If we are not interested in distances over 300 kilometers, or if other instrumental and propagational limitations prevent us from utilizing the method up to such distances, then we can send 1,000 pulses per second, and obtain, by superposition of the successive images on a synchronized time base, a very easily visible sustained image permitting close measurement and even showing the advance of the craft. Some compromise pulse-frequency between 50 and 1,000 would be selected after experimental trials.

8. It will be clear that the installation of three such receivers for time-delay measurement alone would enable the equations of position to be solved, by means which could be made partially or wholly automatic, for height and plan projection. The provision of a line of senders over a long front is not prohibitively difficult, since the polar diagrams are such as to permit substantial spacings and the echo patterns are readily sorted out. Finally the provision of two parallel lines, roughly perpendicular to expected line of approach, would give still-more-accurate positional data enabling speed and course to be measured with some precision. There are two main objections to the use of the radio frequencies discussed, to which the whole metal structure of the craft is nearly resonant. The technical one is that echoes from the ionosphere will appear on the received picture and will have to be discounted in observation. This is no more than a mere inconvenience, in view of our existing knowledge of what to expect, and even this inconvenience is mitigated by the value of the ionospheric echoes as indicators that the gear is in good order. The time scale can be made very open for the first 100 kilometers—and it is not unreasonable to expect that the technique can be developed to operate on craft up to that distance—and the first ionospheric echoes can be crowded into a standstill period at the end of the time base. But it is impossible to avoid the ionospheric echoes from, say (nk + x) km. being read as from x km., where k is the distance corresponding to the recurrence frequency of the time base and n = 1, 2, 3, . . . , except by the exercise of intelligence and experience of ionospheric reflection, or by additional instrumental artifices.

9. The second objection is one of policy. The ionospheric reflection makes it certain

that these special emissions will be audible in foreign countries, and alike on grounds of secrecy and of mitigating interference with communications this is undesirable. The interference problem can, presumably, be dealt with through the normal machinery, with due regard to the importance of the objective. The secrecy problem might be best solved by an offer from Air Ministry to Department of Scientific and Industrial Research of Facilities for ionsopheric investigation and other work for the Radio Research Board at a conveniently flat and isolated site at Orfordness, suitably distant from Slough for special experiments.

10. It is felt that none of these objections should be allowed to delay the attack which depends on the use of the wave lengths, around 50 meters, on which we have adequate experience and adequate radiated power. But as soon as possible the technique should be developed to cover the wave lengths under 10 meters, which are not normally reflected from the ionosphere, and which would thus mitigate the interference problem and would help to maintain secrecy after the "camouflage" already suggested were beginning to wear thin.

11. The power which can at present be radiated on these shorter wave lengths is about half that attainable in the 50 meter range, and the receivers are probably somewhat less sensitive, so that some sacrifice of sensitivity would at first result. The main reason for preferring the 50-meter wave length, however, is connected with means, for location by reflected pulse signals, other than by the measurement of time delay as already outlined.

12. The cathode-ray direction finder, developed at Slough for visual direction finding on extremely brief signals, has already been used on 50 meters, but not yet on 10 meters. It is almost certain that instruments of this type, working on 50 meters, could be used at the ends of a suitable baseline, the indications being "piped" to a central control room in which the advance of the craft could be indicated continuously by the movement, on a map, of the point of intersection of two lines of light representing the directly indicated bearings at the two stations.

13. This technique can doubtless be extended to 10-meter working, but substantial development work is yet required. Closely related experiments down to 15 meters have, however, revealed no acute difficulties.

14. It may, further, be desirable to supplement or supplant the time-delay measurements by adding to the cathode-ray technique also worked out (exclusively as was the direction finder) at Radio Research Station, Slough. This enables the angle of elevation of descending radio waves to be measured with an accuracy of about half a degree, an accuracy which can almost certainly be improved on demand; the work already in hand has not required higher accuracy. This technique has already been used on wave lengths between 60 meters and 10 meters.

15. The manner in which the three methods may best be combined for the most rapid deduction of the most convenient positional co-ordinates from these direct and continuous indications of the distance, angular azimuth, and angular elevation of the craft can be determined by trial and development.

16. I am, however, convinced that the work can be brought to a successful issue only by the utilization of the wide range of cathode-ray technique in which Radio Research Station, Slough, has specialized for many years, and in which its experience is unique.

17. If the foreseen difficulties of the pulse method prove unexpectedly great, or if some major difficulty has not been foreseen, there remain two practicable though less attractive processes. In one the sender would emit continuous-wave signals, and no echo would be detected save from a moving reflector, such as the craft. The rate of approach could be measured from the interference pattern on the cathode-ray screen, the plan position could be plotted from cathode-ray direction finders into which were injected suitably phased electromotive forces to suppress the images due to the direct rays and those reflected from fixed objects.

18. In the other process the frequency of the sender would be varied over a known

range, as in Appleton's frequency-change method of ionospheric sounding. Here the interpretation of the pattern from a moving reflector would appear likely to be slower than is permitted by the practical problem of locating–and intercepting–high-speed enemy craft, and the method is not proposed for consideration until some flaw has been found in the quite unexpectedly favorable indications for the pulse method.

19. There will also be, for consideration, the problem whether the interval between detection and engagement may not be best reduced to a minimum by having interceptor craft fitted with a keyed resonating array so that they are readily located by the same methods as those used on the enemy bombers, but discriminated and identified by the intermissions in their "reflected" field. The interception operation can then be controlled by radio instructions to the interceptors closing them into the positions indicated for the bombers.

20. We have already disclosed, in patents and publications, means for making the oscillographs "follow up" and these may be relevant to further development of the present scheme, as for distant repeating, etc.

THE ENVIRONMENT OF THE ELECTROMAGNETIC CONFLICT

Since the electromagnetic conflict occurs as a part of a larger national conflict, it is important to understand some of the associated factors which bear on that conflict. In so doing it becomes clear that there are two basic situations, wartime and peacetime—or using current euphemisms, hot and cold war. The major difference between these two situations is the presence or absence of open armed conflict between adversaries, and this difference has a major impact on the conduct of the electromagnetic conflict.

Much of what we have to say is in one sense well known, for any commander realizes that his role in national confrontation changes between war and peace. What we propose to do is cast the major relationships into a structural framework compatible with systems dynamics. This approach may seem strange to some but we want to emphasize the closed-loop character of the relationship between the different elements comprising combat capability with its potential for a wide variety of behavior, that is, the wide variety of outcomes we observe in history.

But this potential does not arise solely because of external factors, rather the closed-loop approach emphasizes the interaction between the various elements of the structure as the source of dynamic behavior. In turn, this interaction depends on both the functional relationships embodied in the elements of the structure and the relative magnitudes of the variable quantities in the model. Experience with other systems dynamics models suggests three rules of thumb for these complex systems. First, the variety of interactions can be expressed as a change in the dominance of the various loops of the model. Second, in general the behavior is insensitive to most of the internal parameters. And third, the important parameters are not always intuitively obvious. This latter idea has led some systems to be labelled "counterintuitive".[1]

Unfortunately, it is impossible at the present time to determine the dominant loops in any particular situation and the important parameters without setting up such a model and running it on a computer. To the best of our knowledge this has not been done for a national conflict model, yet without such detailed knowledge this model still seems to be useful as a quasi-precise method of stating the structural relationships between the different elements involved in military conflict. Hence it does appear useful in gaining an understanding of how the electromagnetic conflict influences the rest of warfare.

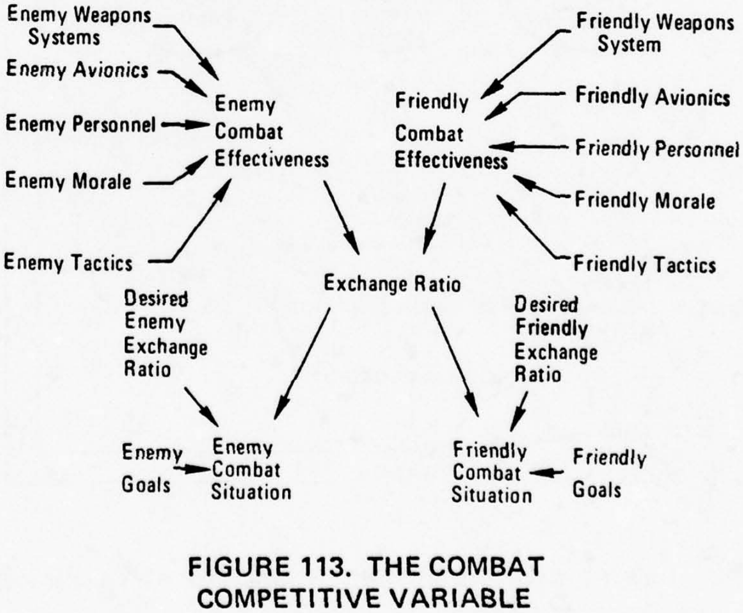


FIGURE 113. THE COMBAT COMPETITIVE VARIABLE

[1] Jay W. Forester, "Counterintuitive Behavior of Social Systems", *Technology Review 73* (January 1971).

The Wartime Structure

If the structure of conflict has a closed-loop character and is goal-seeking then there must be some measure of effectiveness which the commander can use to decide if the outcome is favorable. We propose that an appropriately defined exchange ratio, as preceived by the commander, is that measure of effectiveness. This exchange ratio is the ratio of the enemy resources captured or destroyed to the friendly resources lost in an engagement. That is,

$$\text{Exchange Ratio} = \frac{\text{Enemy ResourcesCaptured or Destroyed}}{\text{Friendly Resources Lost}} \qquad (22)$$

In turn, the exchange ratio is dependent upon the relative combat effectiveness of the two opposing sides. And combat effectiveness is in turn dependent on the weapons systems, electronics (avionics in an airborne context)[2], personnel, tactics and morale of the two sides.

However, the exchange ratio is not the only measure of effectiveness. Besides comparing the actual exchange ratio with his desired exchange ratio, the commander will consider the movement of the FEBA, the losses to supporting ground troops and other factors in assessing his relative combat position. Hence, when we draw out the structure as in Figure 113 we must add the exogenous input "goals" to account for these factors.

Let us consider each of the components of combat effectiveness. Since the friendly and enemy systems are in principle similar (having the same basic structure) we shall consider only the friendly system. (If our purpose were not conceptual exposition but simulation we would want to consider in more detail any differences between friend and enemy.) Our conceptualization of the military system is that it contains the five major feedback loops shown in Figure 114 (see also Figure 21). We shall discuss the composition of each loop in turn.

Weapons System. The basic structure of the weapons system loop is shown in Figure 115. An undesirable combat situation triggers a requirement for better capability in the area of weapons systems. This requirement can be satisfied either by withdrawing systems from stockpiles, buying more of existing weapons systems or by developing new systems. The decision to withdraw from stockpile is influenced only by present stockpile level and it incurs a delay of only a few months. A decision to procure existing weapon systems is influenced by the existence of production facilities and the budget; but the decision having been made to do so, a delay of 1 to 2 years may be incurred

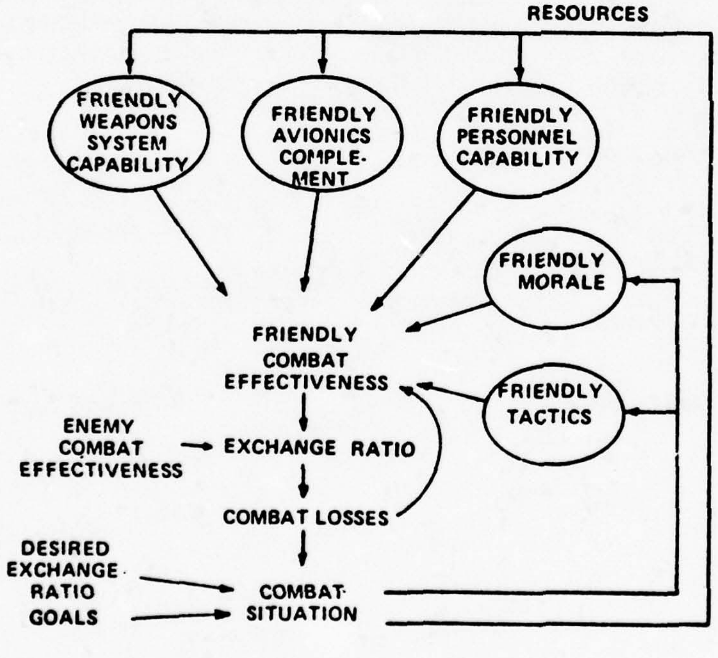

RESOURCES
FRIENDLY WEAPONS SYSTEM CAPABILITY
FRIENDLY AVIONICS COMPLE-MENT
FRIENDLY PERSONNEL CAPABILITY
FRIENDLY MORALE
FRIENDLY COMBAT EFFECTIVENESS
FRIENDLY TACTICS
ENEMY COMBAT EFFECTIVENESS
EXCHANGE RATIO
COMBAT LOSSES
DESIRED EXCHANGE RATIO
GOALS
COMBAT SITUATION

FIGURE 114. THE FRIENDLY MILITARY SYSTEM

[2] Avionics is broken out separately because it appears that avionics is one part of every weapons system which can be changed easily. In fact, we commonly see a basic airframe with several different suits of avionics.

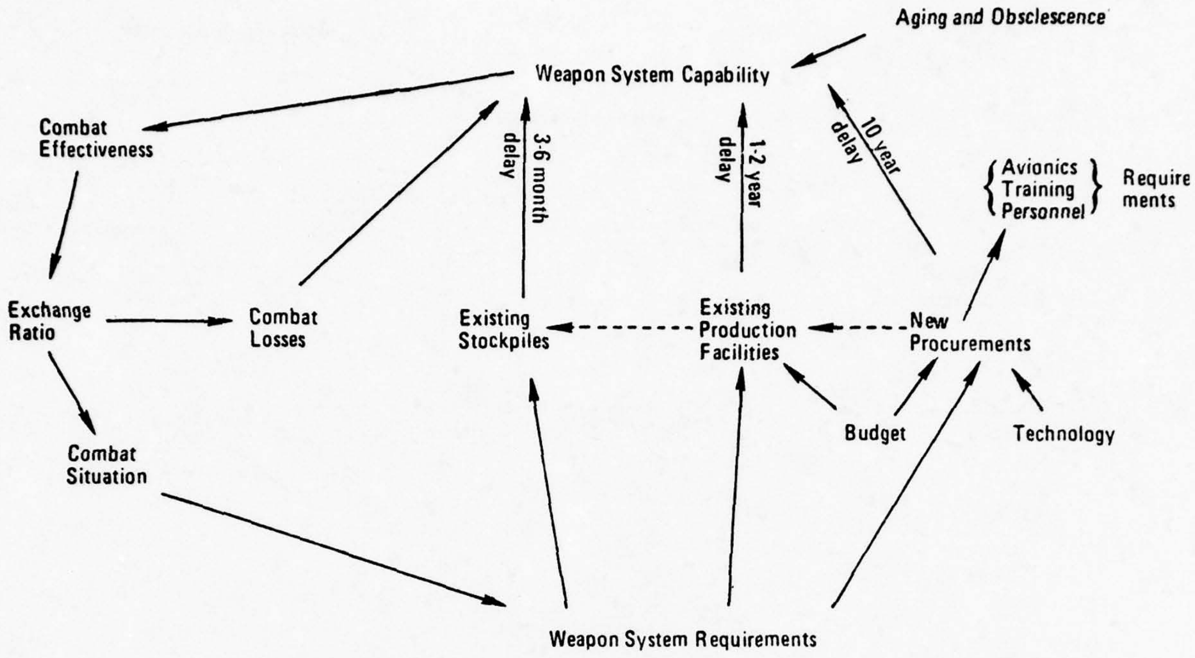


FIGURE 115. THE WEAPON SYSTEM COMPONENT

before the weapon system inventory is affected.

On the other hand, if the decision is to develop a new weapons system, then a required operational capability (ROC) must be written, the system developed, and produced. In this process the projected budget and technology must be considered, and the weapon system development generates new avionics, training and personnel requirements. In addition, production facilities are affected. Overall, this process takes on the order of 10 years to complete.

It should be noted that these loops are basically negative feedback loops in that a decreasing exchange ratio triggers increased weapon system requirements. The increased requirements tend to increase all quantities leading back to the exchange ratio. Note also that weapon system capability is affected by weapon system obsolescence and aging. These exogenous inputs are policy decisions which may in fact be dependent on the exchange ratio, but it has been decided to exclude them from present consideration.

On the other hand the inner loop containing combat losses is a positive feedback loop. For we note that increasing combat effectiveness produces a better exchange ratio which in turn means decreased combat losses, increasing weapon system capability and thus increased combat effectiveness. This positive feedback loop has the potential for growth or decay of the exchange ratio, and thus for victory or defeat. However, the combat effectiveness and exchange ratio relationships are almost certainly nonlinear so these effects can be modified or dominated by the other loops. Consequently, deciding what the dominant behavior is without actually constructing and running a model is impossible.

Avionics. The avionics loop is shown in Figure 116. This diagram is essentially the same as that for weapons systems except for the inclusion of new weapon systems avionic requirements and retrofit. In particular, there is one positive feedback loop containing combat losses and three negative

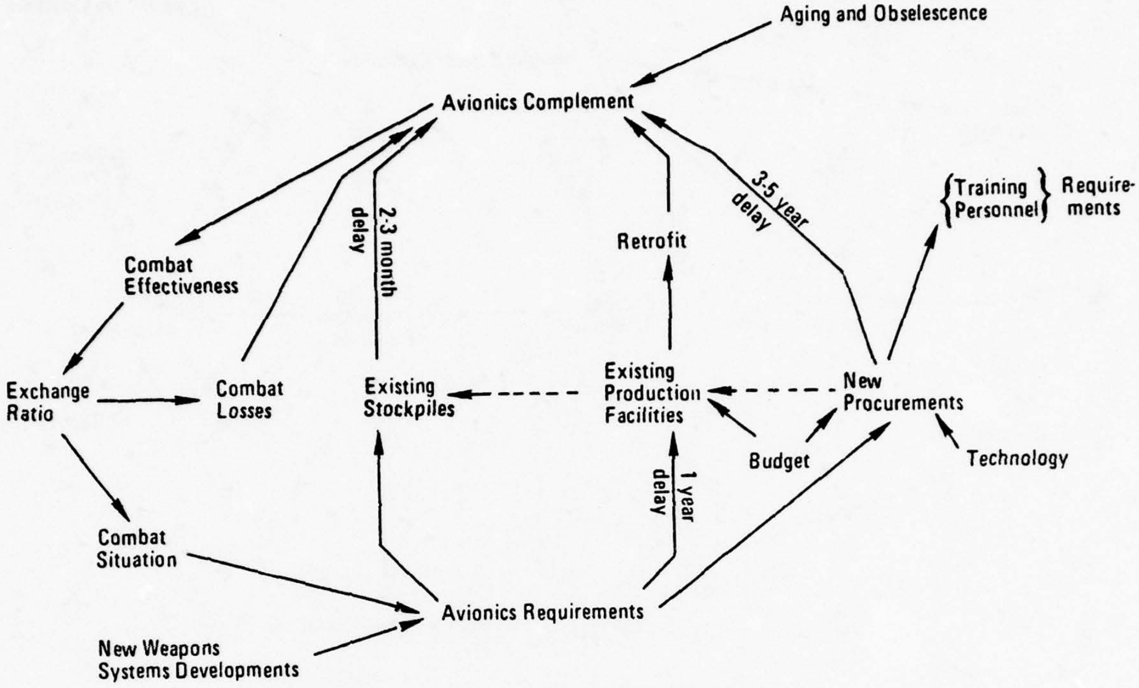


FIGURE 116. THE AVIONICS COMPONENT

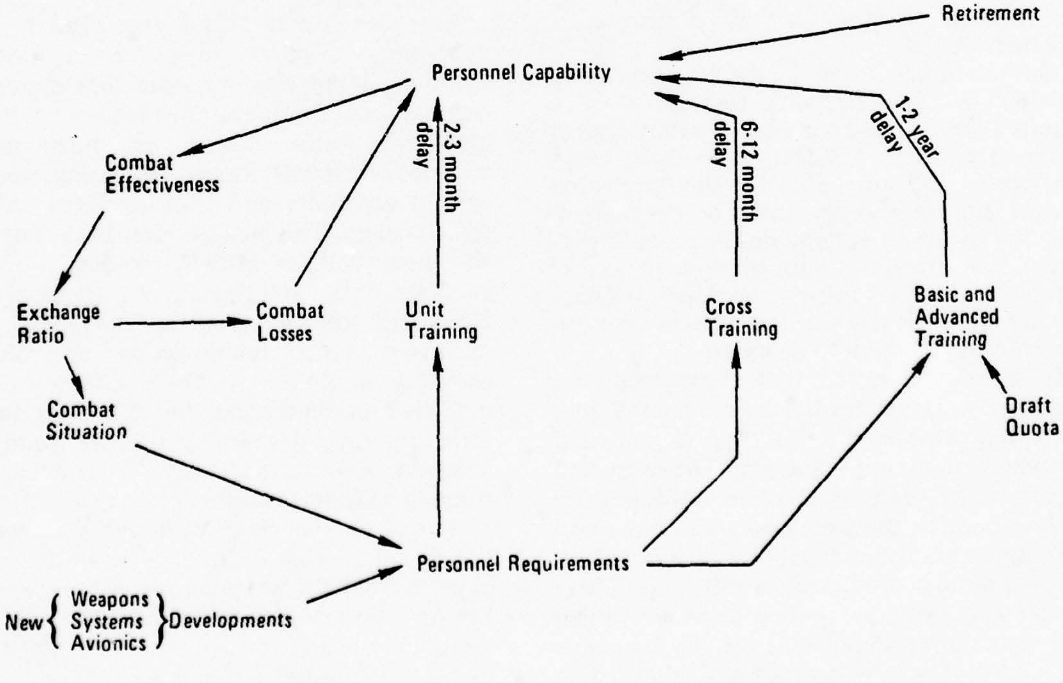


FIGURE 117. THE PERSONNEL COMPONENT

feedback loops. But the delays in the negative feedback loops are shorter because avionics are simpler devices to procure and build.

Personnel. The expansion of the personnel loop is shown in Figure 117. Its structure is similar to that of the two previously discussed loops, but the delays are generally shorter. Unique features of this structure are that personnel requirements are affected by new weapons systems and new avionics through their training requirements while retirement and draft quotas affect personnel capability. Again there is the combination of one positive and three negative feedback loops with the possibility of changing loop dominance and victory or defeat.

Morale and Tactics. These two loops are portrayed together in Figure 118. In this diagram the combat situation determines the tactics in conjunction with the morale and the weapon, avionics and personnel capabilities. Note that combat losses affect tactics indirectly through their effect on morale and on weapons systems, avionics and personnel. The tactics loop is a positive feedback loop since an improvement in the exchange ratio produces in turn an improved combat situation, an increased selection of tactics, improved combat effectiveness and consequently further improvement in the exchange ratio.

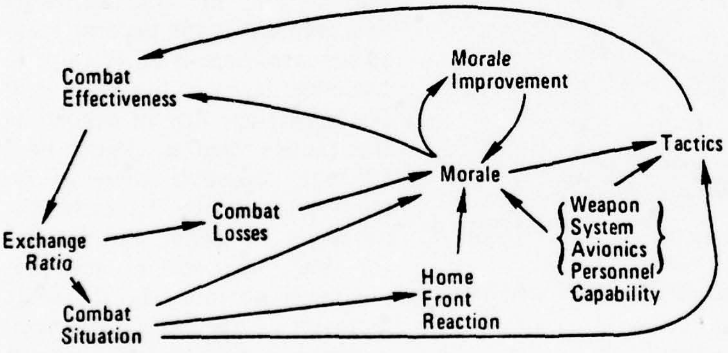


FIGURE 118. THE TACTICS AND MORALE COMPONENTS

On the other hand, the loops containing morale are more complex. In addition to being influenced by the combat situation, combat losses, and the weapons system, avionics and personnel capability, morale is also influenced by the home front reaction to the war and by morale improvement efforts of the commander. Since the goal of morale improvement is high morale, then the loop containing morale improvement is a negative feedback or goal-seeking loop. But the loops containing combat losses and home front reaction may be either positive or negative feedback depending upon the perceived objectives of the conflict; in any case these loops are likely to be highly nonlinear. Thus the overall effect of the morale loops is difficult to ascertain in general.

In spite of the difficulty of determining the relative character and dominance of these two loops, it seems clear that both loops can have very short delays, from hours to a few days. Thus the commander can use these elements of the conflict as immediate remedies to an unfavorable situation. Whether or not he is successful may depend on the other loops and on circumstances, for they determine if the effects achieved through these loops can be sustained.

Recapitulation. It is clear that the structure influencing the commander's management of his forces is complex. Furthermore, the presence of both positive and negative feedback loops allows for growth and decay–winning or losing the battle–and for a variety of dynamic behavior. Because the range of time delays is wide the interaction of. the loops can be very complex. However we can make the following observations.

1. Except for extended tactical campaigns (greater than 3 years) the weapon system and avionics development loops are not contributors to the dynamics due to their long delays.

2. Weapon system and avionics stockpiles and the

loops dependent on them only affect the conflict in the beginning phases of a campaign, or at the beginning of a radical change in tactics. Likewise, procurement of existing weapon systems and avionics is not effective policy for short campaigns unless the facilities are available.

3. Hence the effect of the weapon systems and avionics loops on the conflict are very dependent on the initial conditions at combat inception for short campaigns. For long campaigns they could have a significant impact.

4. The tactical commander must generally rely upon his personnel, their morale, and tactics to influence the battle in the short run.

5. The best strategy for avionics and weapon system development in peacetime would seem to be to build up stockpiles so that the tactical commander has a large number of options at his disposal at the beginning of hostilities.[3]

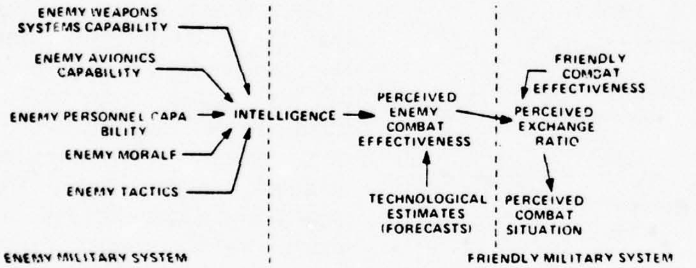

ENEMY WEAPONS SYSTEMS CAPABILITY
ENEMY AVIONICS CAPABILITY
ENEMY PERSONNEL CAPA BILITY
ENEMY MORALE
ENEMY TACTICS
INTELLIGENCE
PERCEIVED ENEMY COMBAT EFFECTIVENESS
TECHNOLOGICAL ESTIMATES (FORECASTS)
FRIENDLY COMBAT EFFECTIVENESS
PERCEIVED EXCHANGE RATIO
PERCEIVED COMBAT SITUATION
ENEMY MILITARY SYSTEM
FRIENDLY MILITARY SYSTEM

FIGURE 119. THE PEACETIME COMPETITIVE VARIABLE

6. The preponderance of negative feedback loops means that much of the system is insensitive to many parameters. However, it is also true that the length of the delay in the various loops is a significant parameter.

The Peacetime Structure

The previous discussion has been set in the context of open national conflict, but what provides the impetus for weapon system development in peacetime? We hypothesize that an inferred exchange ratio is substituted for the directly observed exchange ratio. This inferred exchange ratio is derived from intelligence information on the enemy capability, morale and tactics as diagrammed in Figure 119 (see also Figure 22). Since intelligence is insufficient to give a complete picture of the enemy capability, technological forecasts are employed to round out the picture. However, these forecasts are usually founded on a very narrow base because, lacking the ability to anticipate the enemies' decisions, we attempt to bound his capability with our best estimates of what we *could* do. Thus the system tends to be driven by extreme estimates (the 10-foot-tall enemy). These estimates affect the long delay loops most since they are so sluggish.[4] One result is the recurring mania for weapon sophistication.

Another consequence of peacetime development is that the delays in the hardware procurement loops become longer because there is an attempt to optimize design in the absence of confrontation. For in peacetime the tactics loop is almost nonexistent. Likewise there is no sense of urgency to drive the other loops. Hence the penalty for long procurement delays is not really obvious, and the delay increases. Speaking picturesquely, our military muscles get flabby.

On the basis of the above discussion, one can see the need for:

[3] Unfortunately, building up stockpiles also increases the risk of having large quantities of obsolete weapons on hand at the beginning of a open conflict.

[4] The long delay means that the adequacy of the proposed development will not be known for a long time. Thus a long range forecast is required, but long range forecasts are very likely to be grossly inaccurate so that the utility of the weapon system so developed is likely to be much different than anticipated. Furthermore, loops containing long delays tend to amplify their inputs (the estimates) with their fluctuations. See Forrester, *Industrial Dynamics*, pp 348-349, for a more comprehensive discussion of this point.

1. Extensive intelligence in peacetime to keep our estimates of enemy capabilities reasonable.

2. Extensive training with simulated enemy tactics in peacetime to keep our estimates of the exchange ratio realistic.

3. Evolutionary weapon development. If we always attempt great leaps forward we lose contact with a realistic appraisal of our combat capability versus the enemy's. This is not to say that radical weapon developments have no place, but successive radical developments without combat experience leave no basis for judgment of relative worth.

It is this environment that surrounds and permeates the electromagnetic conlfict in times of peace. Since the various aspects of this conflict are very reactive it is not surprising that this conflict sometimes assumes the most perverse aspects of national conflict. To this is added the general aura of mystery which often pervades this subject in the minds of decision makers and which this book attempts to dispel. Thus it becomes doubly important that we recognize the nature and importance of this conflict that we might be prepared to excell in the future.

APPENDIX F

GLOSSARY FOR ELECTRONIC WARFARE

In a field which is as dynamic as electronic warfare the meaning of terms tend to change with time. Thus any attempt at standardized definitions will always have to face dissenters. The previous text has tried to use terms in their standard meanings wherever such meanings could be established. It appears useful to have a collection of such terms in one place for quick reference, yet we do not want to write a dictionary. Hence, we have extracted definitions from official sources and added others as seemed to be necessary to construct a glossary. As a result there may be differences between the usage given here and that in the text. Such differences are not because of an intentional purpose to contravene existing official definitions but have arisen out of an attempt to clarify concepts.

Many of these definitions have been taken from Air Force Manual 11-1, volumes I and III. In that manual the areas of applicability of certain standardized definitions are given. We have retained that feature through the use of symbols in parenthesis. The meanings of the symbols are as follows:

a. (AF)–Standardized for use within the US Air Force only.

b. (DOD)–Standardized for use within the Joint Services and Department of Defense.

c. (ASCC)–Standardized for use by the American, Australian, British, Canadian, and New Zealand Air Forces.

Since acronyms are commonly used for many of the terms in this glossary we have added a separate listing of acronyms and abbreviations at the end of the glossary.

DEFINITIONS

Acoustic Jamming–(DOD) The deliberate radiation or reradiation of mechanical or electro-acoustic signals with the objectives of obliterating or obscuring signals which the enemy is attempting to receive and of deterring enemy weapons systems.

Acquire–(DOD)

1. When applied to acquisition radars, the process of detecting the presence and location of a target in sufficient detail to permit identification.
2. When applied to tracking radars, the process of positioning a radar beam so that a target is in that beam to permit the effective employment of weapons.

Active Electronic Warfare–The radiation of electromagnetic energy to impair the enemy's use of his electronic sensors or to mislead the enemy in the interpretation of data received from his electronic sensors.

Active Homing Guidance–(DOD) A system of homing guidance wherein both the source for illuminating the target, and the receiver for detecting the energy reflected from the target as the result of illuminating the target, are carried within the missile.

Airborne Early Warning–(DOD) The detection of enemy air or surface units by radar or other equipment carried in an airborne vehicle and the transmitting of a warning to friendly units.

Airborne Early Warning and Control–(DOD) Air surveillance and control provided by airborne early warning vehicles which are equipped with search and height finding radar and communications equipment for controlling weapons.

Airborne Intercept Equipment–(DOD) A fire control system, including radar equipment, installed in interceptor aircraft used to effect air interception.

Airborne Radio Direction Finding–(AF) A technique for precisely locating enemy communications emitters by establishing a fix based on determining their direction from two or more known listening points.

Airborne Warning and Control System–(AF) An aircraft suitably equipped to provide an airborne control, surveillance and communications capability for strategic defense and/or tactical air operations.

Air-Breathing Missile–(DOD) A missile with an engine requiring the intake of air for combustion of its fuel, as in a ramjet or turbojet. To be contrasted with the rocket missile, which carries its own oxidizer and can operate beyond the atmosphere.

Air Defense–(DOD) All defensive measures designed to destroy attacking enemy aircraft or missiles in the earth's envelope of atmosphere, or to nullify or reduce the effectiveness of such attack.

Air Defense Artillery–(DOD) Weapons and equipment for actively combating air targets from the ground. Weapons are classed as:
Light – 20-57mm
Medium – 58-99mm
Heavy – 100mm or greater.

Air Interception–(DOD) To effect visual or radar contact by a friendly aircraft with another aircraft. Normally the air intercept is conducted in the following five phases:

a. *Climb Phase*–Airborne to cruising altitude;

b. *Maneuver Phase*–Receipt of initial vector to target until beginning transition to attack speed and altitude;

c. *Transition Phase*–Increase or decrease of speed and altitude required for the attack;

d. *Attack Phase*–Turn to attack heading, acquisition of target, completion of attack, and turn to breakaway heading; and

e. *Recovery Phase*–Breakaway to landing.

Air-To-Air Missile–(DOD) A missile launched from an airborne carrier at a target above the surface.

Air-To-Surface Missile–(DOD) A missile launched from an airborne carrier to impact on a surface target.

Amplitude Modulation–A method of impressing a message upon a carrier signal by causing the carrier amplitude to vary proportionally to the message waveform.

Amplitude Shift Keying–A method of impressing a digital signal upon a carrier signal by causing the carrier amplitude to take different values corresponding to the different values of the digital signal.

Antenna Sidelobes–The ability of an antenna to receive energy from other directions widely separated from the preferred direction of reception.

Anti-Jamming–A synonym for electronic counter-countermeasures.

Antiradiation Missile–(DOD) A missile which homes passively on a radiation source.

Area Defense–(AF) Area defense involves the concept of locating defense units to intercept enemy attacks remote from and without reference to individual vital installations, industrial complexes, or population centers.

Area Target–(DOD) A target consisting of an area rather than a single point.

Armed Reconnaissance–(DOD) A mission with the primary purpose of locating and attacking targets of opportunity, i.e., enemy materiel, personnel, and facilities, in assigned general areas or along assigned ground communications routes, and not for the purpose of attacking specific briefed targets.

Authentication–(DOD) A security measure designed to protect a communications system against acceptance of a fradulent transmission or simulation by establishing the validity of a transmission, message, or originator.

Automatic Direction Finder–(ASCC) A radio receiver which indicates automatically and continuously the great circle direction to the radio transmitter to which it is tuned.

Automatic Frequency Control–Circuits in a receiver which automatically correct the local oscillator frequency to prevent receiver drift in tuned frequency.

Automatic Gain Control–

1. A circuit used to maintain the output volume of a receiver constant, regardless of variations in the signal strength applied to the receiver.
2. A self-acting compensating device which maintains the output of a transmission system constant within narrow limits in the face of wide variations in the attenuation of the system.
3. A radar circuit which prevents saturation of the radar receiver by long blocks of received signals, or by a carrier modulated at low frequency.

Ballistic Missile–(DOD) Any missile which does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated.

Ballistic Missile Early Warning System–(DOD) An electronic system for providing detection and early warning of attack by enemy intercontinental ballistic missiles

Barrage Jamming–(DOD) Simultaneous electronic jamming over a broad band of frequencies.

Beacon–(DOD) A light or electronic source which emits a distinctive or characteristic signal used for the determination of bearings, courses, or location.

Beam Rider–(DOD) A missile guided by an electronic beam.

Beam Width–(DOD) The angle between the directions, on either side of the axis, at which the intensity of the radio frequency power drops to one-half the value it has on the axis.

Beat Frequency Oscillator–(AF) An oscillator which produces a desired frequency by combining two other frequencies. The frequency may be an audio frequency produced by combining two radio frequencies, or it may be some desired radio frequency, such as the intermediate frequency of a superheterodyne circuit.

Blind Range–Ranges at which pulse-doppler radars produce no output.

Blind Speed—Radial velocities for which pulse radars with MTI signal processors produce no output.

Blip—The spot of light on a radar display which represents a radar echo from an.aircraft.

BOMARC—(DOD) A long-range, surface-to-air guided missile with nuclear warhead for area air defense, powered by twin ramjet engines with either liquid or solid rocket boosters. and terminal guidance. Designated as CIM-10.

Bomber—

1. LIGHT: A bomber designed for a tactical operating radius of under 1,000 nautical miles at design gross weight and design bomb load.
2. MEDIUM: A bomber designed for a tactical operating radius of between 1,000 to 2,500 nautical miles at design gross weight and design bomb load.
3. HEAVY: A bomber designed for a tactical operating radius over 2,500 nautical miles at design gross weight and design bomb load.

Carrier Frequency—Frequency of an unmodulated radio wave emanated from a radio, radar, or other type transmitter.

Cathode-ray Tube—(AF) A vacuum tube in which the instantaneous position of a sharply focused electron beam, deflected by means of electrostatic and/or electromagnetic fields. is indicated by a spot of light produced by the impact of the electrons on a flourescent screen at one end of the tube.

Chaff—(AF) Radar confusion reflectors which consist of thin, narrow metallic strips of various lengths and frequency responses, used to reflect echoes for confusion purposes.

Circular Error Probable—(DOD) An indicator of the delivery accuracy of a weapon system, used as a factor in determining probable damage to a target. It is the radius of a circle within which half of the missiles/projectiles are expected to fall.

Clutter—(DOD) Permanent echoes, cloud, or other atmospheric echoes on radar scope.

Coherent Repeater Jammer—A jammer that uses the phase information of the received radar signal in creating false targets.

Combat Air Patrol—(DOD) An aircraft patrol provided over an objective area, over the force protected, over the critical area of a combat zone, or over on air defense area. for the purpose of intercepting and destroying hostile aircraft before they reach their target.

Command and Control—(DOD) The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission. Command and control functions are performed through an arrangement of personnel, equipment. communications, facilities. and procedures which are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of his mission.

Command Guidance—(DOD) A guidance system wherein intelligence transmitted to the missile from an outside source causes the missile to traverse a directed flight path.

Communication deception--(DOD) Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

Communications Intelligence–(DOD) Technical and intelligence information derived from foreign communications by other than the intended recipients.

Communications Security–(DOD) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes: (1) cryptosecurity; (2) transmission security; (3) emission security; and (4) physical security of communications security material and information.

a. *Cryptosecurity*–The component of communications security which results from the provision of technically sound cryptosystems and their proper use.

b. *Transmission security*–The component of communications security which results from all measures designed to protect transmissions from interception and exploition by means other than cryptanalysis.

c. *Emission security*–The component of communications security which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems.

d. *Physical security*–The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by being within a friendly power.

Conical Scan–A type of scanning in which the axis of the RF beam is titled away from the axis of the reflector and rotated about it, thus generating a cone.

CONSOL–(DOD) A long range radio aid to navigation, the emissions of which, by means of their radio frequency modulation characteristics, enable bearings to be determined.

Constant False Alarm Rate Receiver–A radar receiver with automatic detection circuits designed to produce a constant number of erroneous target detections independent of noise level at the receiver input.

Control of Electromagnetic Radiation--(DOD) A national operational plan to minimize the use of electromagnetic radiation in the United States, its possessions, and the Panama Canal Zone in the event of attack or imminent threat thereof, as an aid to the navigation of hostile aircraft, guided missiles, or other devices.

Continuous Wave–

1. An unmodulated radio transmission.
2. A non-pulsed radio transmission.

Cosecant Squared Antenna–A fan beam antenna which has been modified to radiate more energy at higher elevation angles. This antenna has the property that the echo power received from a constant cross section target at constant altitude is independent of range.

Cross-tell–see *Track Telling.*

Cryptanalysis–(DOD) The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.

Data Link–(DOD) A communications link suitable for transmission of data.

DECCA–(ASCC) A radio phase-comparison system which uses a master and slave stations to establish a hyperbolic lattice and provide accurate position-fixing facilities. (Decca operates in the 70 to 130 kHz frequency band and has an operational range of about 250 miles.)

Deceiver–An ECM equipment which attempts to deceive or mislead a radar by emitting a pulse-like signal similar to the radar signal.

Deception–See Electronic Deception, Imitative Deception, or Manipulative Deception.

Decibel–A unit used to express the ratio between two amounts of power. One decibel is equivalent to a power ratio of 1.26, i.e., to a power ratio whose common logarithm is 0.1.

Decrypt–(DOD) To convert encrypted text into its equivalent plain text by means of a cryptosystem. (This does not include solution by cryptanalysis.) Note: The term decrypt covers the meanings of decipher and decode.

Diplexing–The operation of a radar set on two frequencies simultaneously through a single antenna.

Direct Current–An unvarying current (or voltage). The acronym DC is often used as a synonym for zero frequency.

Direction Finding–(DOD) A procedure for obtaining bearings of radio frequency emitters with the use of a highly directional antenna and a display unit on an intercept receiver or ancillary equipment.

Doppler Radar–(DOD) A radar system which differentiates between fixed and moving targets by detecting the apparent change in frequency of the reflected wave due to motion of target or the observer.

Duplexer–An electronic switch which alternately connects a radar antenna to the radar transmitter and radar receiver.

Early Warning–(DOD) Early notification of the launch, or approach, of unknown weapons or weapons carriers.

Electromagnetic intrusion–(DOD) The intentional insertion of electromagnetic energy into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

Electromagnetic Pulse–An electromagnetic signal produced by ordinary chemical and nuclear detonations. In the case of nuclear detonations, the electromagnetic pulse energy spectrum is continuous with most of the energy distributed throughout the VLF band. See *Nuclear Effects*.

Electromagnetic Radiation–(DOD) Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light. Includes gama radiation, X-rays, ultraviolet, visible and infrared radiation, and radar and radio waves.

Electromagnetic Spectrum–(DOD) The frequencies (or wave lengths) present in a given electromagnetic radiation. A particular spectrum could include a single frequency or a wide range of frequencies.

Electromagnetic Test Environment–(AF) A range complex of radars at Eglin Air Force Base, Florida, operating in different frequency bands and modes to provide a very flexible test facility for evaluating aircraft antenna patterns, reflectivity measurements, infrared, reconnaissance, airborne interceptors, and electromagnetic warfare devices and techniques.

Electronic Counter-Countermeasures–(DOD) That division ofelectronic warfare involving actions taken to insure friendly effective use of the electromagnetic spectrum despite the enemy's use of electronic warfare.

Electronic Countermeasures–(DOD) That division of EW involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Electronic countermeasures include electronic jamming and electronic deception.

Electronic Deception–(DOD) The deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic radiations in a manner intended to mislead an enemy in the interpretation of or use of information received by his electronic systems. There are two categories of electronic deception: (1) *Manipulative deception*–The alteration or simulation of friendly electromagnetic radiations to accomplish deception. (2) *Imitative deception*–The introduction of radiations into enemy channels which imitate his own emissions.

Electronic Intelligence–(DOD) The intelligence information product of activities engaged in the collection and processing, for subsequent intelligence purposes, of foreign, noncommunications, electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

Electronic Jamming–(DOD) The deliberate radiation, reradiation, or reflection of electromagnetic signals with the object of impairing the use of electronic devices, equipment, or systems being used by the enemy.

Electronic line of sight–(DOD) The path traversed by electromagnetic waves which is not subject to reflection or refraction by the atmosphere.

Electronic Order of Battle–A listing of all the electronic radiating equipment of a military force giving location, type, function and other pertinent data.

Electronic Reconnaissance–(DOD) The detection, identification, evaluation, and location of foreign, electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.

Electronics Security–(DOD) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar.

Electronic Warfare–(DOD) Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. There are three divisions within electronic warfare: electronic warfare support measures, electronic countermeasures and electronic counter-countermeasures.

Electronic Warfare Support Measures—(DOD) That division of electronic warfare involving actions taken to search for, intercept, locate, and identify immediately radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support measures provide a source of information required for immediate action involving electronic countermeasures, electronic counter-countermeasures, avoidance, targeting, and other tactical employment of forces.

Electro-optics—(DOD) The interaction between optics and electronics leading to the transformation of electrical energy into light, or vice versa, with the use of an optical device.

Emission Control—Controlling the radiation of an active system such as a radar so that it emits RF energy only when absolutely necessary to perform its mission.

Encrypt—(DOD) To convert plain text into unintelligible form by means of a cryptosystem. (Note: The term encrypt covers the meanings of encipher and encode.)

Extremely High Frequency—Frequencies in the range of 30-300 GHz.

Facsimile—A system of telecommunications for the transmission of fixed images with a view of their reception in a permanent form.

Faker—(DOD) A known strike aircraft engaged in an air defense exercise.

Fast Time Constant—A resistance-capacitance differentiating network with a time constant about equal to the transmitted pulse width and employed in the video portion of the receiver to provide discrimination against jamming with low modulating frequencies.

Filter Center—(DOD) The location in an aircraft control and warning system at which information from observation posts is filtered for further disemination to air defense control centers and air defense direction centers.

Fire Direction Center—(DOD) That element of a command post, consisting of gunnery and communication personnel and equipment, by means of which the commander exercises fire direction and/or fire control. The fire direction center receives target intelligence and requests for fire, and translates them into appropriate fire direction.

Forward Edge of the Battle Area—(DOD) The foremost limits of a series of areas in which ground combat units are deployed, excluding the areas in which the coverning or screening forces are operating, designated to coordinate fire support, the positioning of forces, or the maneuver of units.

Frequency Agility—The ability of a radar to change its transmitted frequency between each transmitted pulse on a pre-planned basis.

Frequency Band Designations—

1. As decided upon by the Atlantic City Radio Convention of 1947 and later modified by Comite Consultatif International Radio (CCIR) Recommendation No 142 in 1953:

Band	*RF Range*
VLF	3-30 kHz
LF	30-300 kHz
MF	300-3000 kHz
HF	3-30 MHz
VHF	30-300 MHz
UHF	300-3000 MHz
SHF	3-30 GHz
EHF	30-300 GHz

2. For electronic warfare use as directed by AFR 55-44:

Band	*RF Range*
A	0-250 MHz
B	250-500 MHz
C	500-1000 MHz
D	1000-2000 MHz
E	2-3 GHz
F	3-4 GHz
G	4-6 GHz
H	6-8 GHz
I	8-10 GHz
J	10-20 GHz
K	20-40 GHz
L	40-60 GHz
M	60-100 GHz

Frequency Diversity–The practice of designing each different type of radar to operate in a different region of the frequency spectrum in order to force potential ECM to cover large regions of the spectrum.

Frequency Modulation–A method of impressing a message upon a carrier signal by causing the carrier frequency to vary proportionally to the message waveform.

Frequency Shift Keying–A method of impressing a digital signal upon a carrier signal by causing the carrier frequency to take different values corresponding to the different values of the digital signal.

Gap Filler–A term applied to radars which are used to fill in "holes" or "gaps" which may exist in the EW radar coverage provided by existing site locations.

Ground-Controlled Intercept–Vectoring an interceptor aircraft to an airborne target by means of information relayed from a ground-based radar site which observes both the interceptor and the target. See *Air Interception.*

Guidance System (Missile)–(DOD) A system which evaluates flight information, correlates it with target data, determines the desired flight path of the missile and communicates the necessary commands to the missile flight control system.

Guided Missile;–(DOD) An unmanned vehicle moving above the surface of the earth, whose trajectory or flight path is capable of being altered by an external or internal mechanism.

Hertz–The unit of frequency, equal to one cycle of variation per second. It supercedes the unit cycle per second (cps).

High Frequency–Frequencies in the range 3000-30,000 kHz.

Home-On-Jam–A method of passive guidance designed to use the jamming signal emitted by the target to track the target in angle.

Homing Guidance–(DOD) A system by which a missile steers itself towards a target by means of a self-contained mechanism which is activated by some distinguishing characteristics of the target.

Identification, Friend or Foe–(DOD) A system using radar transmission to which equipment carried by friendly forces automatically responds, for example, by emitting pulses. thereby distinguishing themselves from enemy forces. It is a method of determining the friendly or unfriendly character of aircraft and ships by other aircraft or ships and by ground forces employing radar detection equipment and associated Identification Friend or Foe units.

Imitative Deception–(DOD) Introducing radiation into enemy channels which imitates his own emmissions.

Infrared–That portion of the frequency spectrum lying between the upper end of the millimeter wave region and the lower (red) end of the visible spectrum. In wavelength the infrared lies between 0.78 and 300 microns, in frequency it lies between 1 and 400 THz.

Infrared Windows–Regions of the infrared frequency spectrum for which the atmosphere is relatively transparent.

Instantaneous Automatic Gain Control–An automatic gain control technique which is characterized by a response time approximately equal to the transmitted pulse width. Some discrimination is achieved against long pulse jamming, extended clutter, and chaff.

Intelligence Cycle–(DOD) The steps by which information is assembled, converted into intelligence, and made available to users. These steps are in four phases:

a. *Direction*–Determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection agencies, and a continuous check on the productivity of collection agencies.

b. *Collection*–The exploitation of sources of information by collection agencies and the delivery of this information to the proper intelligence processing unit for use in the production of intelligence.

c. *Processing*–The step whereby information becomes intelligence through evaluation, analysis, integration, and interpretation.

d. *Dissemination*–The conveyance of intelligence in suitable form (oral, graphic, or written) to agencies needing it.

Intercept Point–(DOD) A computed point in space toward which an interceptor is vectored to complete an interception.

Interceptor–(DOD) A manned aircraft utilized for identification and/or engagement of airborne objects. (An interceptor may or may not be equipped with radar to assist in the interception.)

Intermedicate Frequency–(AF)

1. A fixed frequency to which all carrier waves are converted in a superheterodyne receiver.
2. A frequency to which a signaling wave is shifted locally as an intermediate step during transmission or reception.
3. A frequency resulting from the combination of the received signal and that of the local oscillator in a superheterodyne receiver.

Inverse-Gain Repeater Jammer–A form of repeater in which the jammer creates false targets by varying the output power inversely with the strength of the received radar signal.

Jamming–See Acoustic Jamming, Barrage Jamming, Electronic Jamming or Spot Jamming.

Jamming to Signal Ratio–The inverse of the signal-to-jamming ratio.

Kill Probability–(DOD) A measure of the probability of destroying a target.

Laser Target Designation–(ASCC) The use of a laser to direct a light beam on to the target so that appropriate sensors can track or home on the reflected energy.

Light Amplification by Stimulated Emission of Radiation–(AF) A process of generating coherent light. The process utilizes a natural molecular (and atomic) phenomenon whereby molecules absorb incident electromagnetic energy at specific frequencies, store this energy for short but usable periods, and then release the stored energy in the form of light at particular frequencies in an extremely narrow frequency-band.

Limiter–A device which prevents its output signal from exceeding a predetermined value.

Line of Sight–Electromagnetic wave propagation in straight lines. This term may imply the range limitation imposed by the curvature of the earth upon this mode of propagation.

Lobe–(AF) One of the three-dimensional sections of the radiation pattern of a directional antenna bounded by one or two cones of nulls.

Logarithmic Receiver–A receiver whose response approximates the logarithm of the strength of the incoming signal.

LORAN–(DOD) A long-range radionavigation position fixing system using the time difference of reception of pulse type transmissions from two or more fixed stations.

(Note: 1. LORAN C–An extremely accurate version of LORAN giving accuracies within a few hundred feet for up to 1,000 miles out to sea. Operation is in the band from 90 to 100 kHz. The receiver measures pulse spacing in LORAN fashion to obtain a rough indication of a position, and measures precisely the relative phase of the rf carriers in the master and slave pulse envelopes to refine that position.

2. LORAN D–A tactical LORAN system that uses the coordinate converter of LORAN C in conjunction with the inertial system on an aircraft.)

Low Frequency–Frequencies in the range 30-300 kHz.

Manipulative Deception–(DOD) The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

Matched-Filter Receiver–A radar receiver whose signal processing circuits are designed to discriminate against signals with characteristics different from those of the transmitted rf pulse.

Meaconing–The transmission of false navigation signals with the intent to cause large aircraft navigation errors.

Medium Frequency–Frequencies in the range 300-3000 kHz.

Micron–A unit of length equal to the micro-meter (10^{-6} meter).

Microwave Amplification by Stimulated Emission of Radiation–(AF) A low-noise radio-frequency amplifier. The emission of energy stored in a molecular or atomic system by a microwave power supply is stimulated by the input signal.

Microwave Communications–Normally line-of-sight communications, the frequency of which is higher than 300 MHz.

Modulation–The process of impressing a message-bearing waveform upon another waveform, called the carrier, in such a manner that the message can be recovered (by demodulation or detection).

Monopulse Radar–(AF) A radar using a receiving antenna system having two or more partially overlapping lobes in the radiation patterns. Sum and difference channels in the receiver compare the amplitudes or the phases of the antenna outputs to determine the angle of arrival of the received signal relative to the antenna boresight.

Moving Target Indicator–(DOD) A radar presentation which shows only targets which are in motion. Signals from stationary targets are subtracted out of the return signal by the output of a suitable memory circuit.

Multiplex–Simultaneous transmission of two or more signals on a common carrier wave. The three types of multiplex are called time division, frequency division and phase division.

National Intelligence Estimate–(DOD) A strategic estimate of capabilities, vulnerabilities and probable courses of action of foreign nations which is produced at the national level as a composite of the views of the intelligence community.

Noise–(ASCC) An unwanted receiver response, other than another signal (interference). Noise may be audible in voice communication equipment or visible in equipment such as radar. In the latter case it is also known as *snow*.

Noise Factor–The excess noise added to a signal by an amplifier expressed as the ratio of the noise present with the amplifier to the noise present with the amplifier.

Nuclear Effects–(AF) The electromagnetic phenomena resulting from a nuclear explosion are termed nuclear effects. These phenomena are listed as follows:

1. *Argus Phenomena (Trapped Electrons).* The Argus phenomena is the trapping in the earth's magnetic field of electrons produced by a nuclear burst. These trapped electrons can injure personnel and damage electronic equipment of systems in space.
2. *Blackout*–Radio frequency interference (blackout) is an effect which is the result of ionization produced by a nuclear explosion in or above the atmosphere. This ionization can cause interference (blackout) by attenuating, reflecting, cluttering, and scattering radar and radio signals.
3. *Electromagnetic Pulse.* The nuclear electromagnetic pulse is a high-intensity burst of electromagnetic radiation predominantly in the radio frequency range of the spectrum. It is produced by the asymmetric charge and current distribution occurring about the point of detonation of a nuclear weapon. Electromagnetic pulse is produced in both surface and high altitude bursts.
4. *Optical Phenomena.* Intense radiations covering all parts of the optical spectrum are produced by the interactions between the atmosphere and the nuclear radiation and fission products resulting from a nuclear detonation. The resulting auroras and airglows are created as an optical background which can affect reconnaissance, tracking, warning and homing systems, and personnel.
5. *Transient Radiation Effects on Electronics.* Nuclear radiation impinging on electronic systems or components can substantially alter the operation and output of these systems. The word *transient* refers to the type of environment and not to the duration of the effect since the effect may be either transient or permanent.

Omnirange–(AF) Radio aid to air navigation which creates an infinite number of paths in space throughout 360 degrees azimuth.

Optical countermeasures–(AF) Applications of electronic countermeasures in the visible light portion of the electromagnetic spectrum. Actions taken to prevent or reduce an enemy's effective use of the visible spectrum.

Order of Battle–(DOD) The identification, strength, command structure, and disposition of personnel, units, and equipment of any military forces.

Over-the-Horizon Radar–(AF) A radar system that makes use of the ionosphere to extend its range of detection beyond line-of-sight. Over-the-horizon radars may be either forward scatter or back-scatter systems.

Passive Electronic Countermeasures–Electronic countermeasures based on the reflection, absorption or modification of the enemy's electromagnetic energy. This distinction between active and passive countermeasures is not currently used, but it is based on the presence or absence of an electronic transmitter.

Passive Homing Guidance–(DOD) A system of homing guidance wherein the receiver in the missile utilizes radiation from the target.

Penetration Aids–(AF) Techniques and/or devices employed by aerospace systems to increase the probablity of weapon system penetation of an enemy defense. Examples are: low altitude profiles, trajectory adjustments, reduced radar cross-sections of attack vehicles, improved vehicle hardness to effects of defense engagements, terrain avoidance radar, bomber defense missiles, decoys, chaff, electronic countermeaures, etc. Penetration aids are used by an offensive system to penetrate more effectively enemy defenses. Also called *penaids.*

Phase Modulation–A method of impressing a message upon a carrier signal by causing the carrier phase to vary proportionally to the message waveform.

Phase Shift Keying–A method of impressing a digital signal upon a carrier signal by causing the carrier phase to take different values corresponding to the different values of the digital signal.

Plan-Position Indicator–(AF) A radar indicator in which the signal appears as a bright spot, with range indicated by distance from the center of the screen and bearing by its radial angle.

Point Defense–(AF) Point defense has as its purpose the defense of specified geographical areas, cities, and vital installations. One distinguishing feature of point defense missiles is that their guidance information is received from radars located near the launching sites. See also *Area Defense.*

Point Target–(DOD) A target of such small dimension that it requires the accurate placement of ordnance in order to neutralize or destroy it.

Polarization Diversity–A broad term indicating the use of more than one type of polarization.

PRF Stagger–Interpulse intervals which differ but follow a regular pattern.

Primary Radar–(AF) Radar in which signals are broadcast and the return signals reflected from a target. Contrasted with *Secondary Radar.*

Pulse Compression–A means of operating a radar so as to obtain the resolution and accuracy of a short pulse, but the detection capability of a long pulse. This is accomplished by modulating a long transmitted pulse.

Pulse Duration Modulation–(AF) A form of pulse-time modulation in which the duration of a pulse is varied. Also called *Pulse Length Modulation; Pulse Width Modulation.*

(Note: the modulating wave may vary the time of occurrence of the leading edge, the trailing edge, or both edges of the pulse.)

Pulse Jitter–Random variation of interpulse interval.

Pulse Modulation–(AF)

1. The modulation of a carrier by a pulse train. (Note: In this sense, the term describes the process of generating carrier-frequency pulses.)

2. Modulation of one or more characteristics of a pulse carrier. (Note: In this sense, the term describes methods of transmitting information on a pulse carrier.)

Pulse Position Modulation--Modulation by variation of the interval which elapses between the pulse to be modulated in a group of pulses and a synchronizing pulse, usually the first pulse of the group.

Pulse Repetition Frequency—The rate at which a radar set transmits pulses.

Pulse Repetition Interval—The interval of time between two transmitted radar pulses; the reciprocal of the Pulse Repetition Frequency.

Pulse Width Discrimination—The action of an electronic circuit which measures the pulse length of video signals and passes only those whose time duration lies within set limits.

QUAIL—(DOD) An air-launched decoy missile carried internally in the B-52 and used to degrade the effectiveness of enemy radar, interceptor aircraft, air defense missiles, etc. Designated as AGM-20.

Quadrature—(AF) The expression of the phase relationship between two periodic quantities of the same period when the phase difference between them is ¼ of a period. Also called *Phase Quadrature*.

Quench Frequency—(AF) The number of times per second that a circuit is caused to go in and out of oscillation.

Radar Beacon—(DOD) A receiver-transmitter combination which sends out a coded signal when triggered by the proper type of pulse enabling determination of range and bearing information by the interrogating station or aircraft.

Radar Coverage—(DOD) The limits within which objects can be detected by one or more radar stations. (Note: Radar coverage takes into account aircraft size, altitude, screening angle, site elevation, type radar, antenna radiation pattern and antenna tilt.)

Radar Cross Section—The ratio of the power returned in a radar echo to the power impinging on the target reflecting the signal.

Radar Netting—(DOD) The linking of several radars to a single center to provide integrated target information.

Radar Reconnaissance—(DOD) Reconnaissance by means of radar to obtain information on enemy activity and to determine the nature of terrain.

Radar Silence—(DOD) An imposed discipline prohibiting the transmission by radar of electromagnetic signals on some or all frequencies.

Radiation Intelligence—(DOD) Intelligence derived from the collection and analysis of non-information bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipments, and systems, excluding those generated by the detonation of atomic/nuclear weapons.

Radio Deception–(DOD) The employment of radio to deceive the enemy. Radio deception includes sending false dispatches, using deceptive headings, employing enemy call signs, etc. See also *Electronic Deception.*

Radio Fix–(DOD)

1. The location of a friendly or enemy radio transmitter, determined by finding the direction of the radio transmitter from two or more listening stations.
2. The location of a ship or aircraft by determining the direction of radio signals coming to the ship or aircraft from two or more sending stations, the locations of which are known.

Radio Frequency–(AF) A frequency for which radio transmission is useful for communications purposes. The useful range is from approximately 10 kHz to 300,000 MHz.

Radio Frequency Interference–Unintentional interfering signals present in electronic equipment. Although these signals are designated as radio frequency there is no implication that they are transmitted by electromagnetic radiation through space and enter the equipment through an antenna. Radio frequency interference may enter the equipment through the case or may be conducted along power lines or other wires that enter the equipment.

Range Gate–(AF) A gate voltage used to select radar echoes from a very short range interval.

Range Gate Capture–(AF) An electronic countermeasure technique using a spoofer radar transmitter to produce a false target echo that can make a fire control tracking radar move off the real target and follow the false one.

REDEYE–(DOD) A man-transportable guided missile, fired from the shoulder. designed to provide combat troops with the capability of destroying low-flying aircraft. Designated as XFIM-43A.

Repeater–A receiver-transmitter combination which amplifies the received signal and retransmits it.

Resolution–The ability of a system to distinguish between two adjacent objects and to display them separately.

Rope–(DOD) An element of chaff consisting of a long roll of metallic foil or wire which is designed for broad, low-frequency response.

Saturating Signal–(AF) In radar, a signal of an amplitude greater than the dynamic range of the receiving system.

Scan–(DOD)

1. In air intercept, a term meaning search sector indicated and report any contacts.
2. (ELINT) The motion of an electronic beam through space searching for a target. Scanning is produced by the motion of the antenna or by lobe switching.

Scan Period–(DOD) The time period of basic scan types (except conical and lobe switching) or the period of the lowest repetitive cycle of complex scan combinations. The basic unit of measurement is degrees/mils per second or seconds per cycle.

Scan Type–(DOD) The path made in space by a point on the radar beam, for example; circular, helical, conical, spiral, or sector.

Scientific and Technical Intelligence–(DOD) The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers:

a. foreign developments in basic and applied research and in applied engineering techniques; and

b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and material, the research and development related thereto, and the production methods employed for their manufacture.

Search–(AF)

1. A term applied to that phase of radar operation when the lobe, or beam of radiated energy, is directed in such a way to search for targets in the area.
2. A systematic examination of space to locate and identify targets of interest.

Secondary Radar–(AF) Radar in which the received pulses have been transmitted by a responder triggered by the incident signal. Contrasted with *Primary Radar*.

Selective Identification Feature–(DOD) A capability which, when added to the basic Identification Friend or Foe system, provides the means to transmit, receive, and display selected coded replies.

Self-Screening Range–(AF) The range at which a target can be detected by a radar in the midst of its jamming mask, with a certain specified probability.

Semiactive Homing Guidance–(AF) A system of homing guidance wherein the receiver in the missile uses radiations from a target which has been illuminated by an outside source.

Semiautomatic Ground Environment–(AF) Air defense system in which air surveillance data are processed for transmission to computers at direction centers.

Sensitivity Time Control–A circuit which reduces the gain of the radar receiver immediately following the transmission of the radar pulse so that the receiver is not saturated by strong radar returns from nearby objects.

Sensor–(DOD) A technical means to extend man's natural senses; an equipment which detects and indicates terrain configuration, the presence of military targets, and other natural and manmade objects and activities by means of energy emitted or reflected by such targets or objects. The energy may be nuclear, electromagnetic, including the visible and invisible portions of the spectrum, chemical, biological, thermal, or mechanical, including sound, blast, and earth vibration.

SHORAN–(DOD) A precise short-range electronic navigation system which uses the time of travel of pulse-type transmission from two or more fixed stations to measure slant-range distance from the stations. Also, in conjunction with suitable computer, used in precision bombing.

SHRIKE–(AF) A passive homing air-to-surface anti-radar missile (designed) for use against enemy (gun and missile directing) radars. Designated as AGM-45/A.

Side Lobe Suppression–The suppression of that portion of the beam from a radar antenna other than the main lobe.

Side-looking Airborne Radar–(DOD) An airborne radar, viewing at right angles to the axis of the vehicle, which produces a presentation of terrain or moving targets.

SIDEWINDER–(DOD) A solid-propellant, air-to-air rocket with nonnuclear warhead, and infrared, heat-seeking homer. Designated as AIM-9.

Signal–(DOD)

1. As applied to electronics, any transmitted electrical impulse.

2. Operationally, a type of message; the text of which consists of one or more letters, words, characters, signal flags, visual displays or special sounds, with prearranged meanings and which is conveyed or transmitted by visual, acoustical, or electrical means.

Signal Intelligence–(DOD) A generic term which includes both communications intelligence and electronic intelligence.

Signal Security–(DOD) A generic term which includes both communications security and electronic security.

Signal-to-Jamming Ratio–The ratio of the signal power to the jamming (ECM) power at a particular point in a system. This ratio is often expressed in decibels.

Signal-to-Noise Ratio–The ratio of the signal power to the noise power at a particular point in a system. This ratio is often expressed in decibels.

Skin Paint–A radar echo from an aircraft or the display symbol which indicates that echo, as distinguished from a radar beacon return.

Spoofer–(DOD) In air intercept, means a contact employing electronic or tactical deception measures.

Spot Jamming–The jamming of a specific channel or frequency.

Spurious Radiation–(AF) Emissions from a radio transmitter at frequencies outside of its assigned or intended emission frequency. Spurious emissions include harmonic emissions, parasitic emissions, and intermodulation products, but exclude emissions in the immediate vicinity of the necessary band which are a result of the modulation process for the transmission of information.

Spurious Response–(AF)

1. Any response, other than the desired response, of an electric transducer or device.

2. A term used in electronic warfare to describe the undesirable signal images in the intercept receiver resulting from the mixing of the intercepted signal with harmonics of the local oscillators in the receiver.

Squelch Circuit–(AF) A circuit for preventing a radio receiver from producing audio frequency output in the absence of a signal having predetermined characteristics.

Super High Frequency–Frequencies in the band 3-30 GHz.

Surface-to-Air Missiles—A missile launched from a surface launcher at a target above the surface.

Surveillance—The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means.

7 *Sweep Jamming*—Jamming in which a noise-like signal is moved rapidly and irregularly throughout a frequency band.

Sweep-Lock-on-Jammer—A transmitter in which a narrow-band jamming signal can be tuned over a broad frequency band and the signal locked on a particular frequency.

Tactical Air Navigation—(AF) A short-range ultra-high frequency air navigation system that provides accurate slant-range distance and bearing information. This information is presented to the pilot in two dimensions—that is, distance and bearing from a selected ground station.

Target Acquisition—The detection, identification and location of a target in sufficient detail to permit the effective employment of weapons.

Temperature Scales—Temperature measurement is characterized by two quantities, the size of the unit (1 degree, symbolized by °) and location of zero on the scale. Since the common points of temperature calibration are the melting point of ice and the boiling point of water under standard pressure, the size of the units are specified by the number of degrees between these two temperatures. Two unit sizes may be found, Centigrade with 100 degrees between the ice point and the steam point, and Fahrenheit with 180 degrees between those two points. Absolute temperature scales set their zero at absolute zero, other scales set it near the ice point. The following table compares the temperature scales in common use.

	Fahrenheit	Rankine	Centigrade	Kelvin
	°F	°R	°C	°K
Steam point	212	672	100	373
Ice point	32	492	0	273
Absolute zero	-460	0	-273	0

Terminal Defense—see *Point Defense*

Terminal Guidance(DOD)

1. The guidance applied to a guided missile between midcourse guidance and arrival in the vicinity of the target.
2. Electronic, mechanical, visual or other assistance given an aircraft pilot to facilitate arrival at, operation within or over, landing upon or departure from an air landing or air drop facility.

Terminal Threat—The defense weapon systems used to directly engage a penetrator in order to destroy it.

Terrain-Avoidance Radar—(AF) An airborne radar which provides a display of terrain ahead of a low-flying airplane to permit horizontal avoidance of obstacles.

Terrain-Following Radar—(AF) An airborne radar which provides a display of terrain ahead of a low-flying aircraft to permit manual control, or signals for automatic control, to maintain constant altitude above the ground.

Threshold–(AF) Generally, the minimum value of a signal that can be detected by the system or sensor under consideration.

Time of Arrival–A method of locating a distant pulse emitter by measuring the difference in the time of arrival of its pulses at three separate locations. This method is also called *Inverse LORAN.*

Track–(DOD)

1. A series of related contacts displayed on a plotting board.
2. To display or record the successive positions of a moving object.
3. To lock onto a point of radiation and obtain guidance therefrom.
4. To keep a gun properly aimed, or to point continuously a target locating instrument at a moving target.
5. The actual path of an aircraft above, or a ship on, the surface of the earth. The course is the path which is planned; the track is the path which is actually taken.

Tracking–(AF)

1. The process of keeping a radio beam, or the cross hairs of an optical system, set on a target and determining the range of the target continuously.
2. The maintenance of proper frequency relations in circuits designed to be simultaneously varied by gang operations.
3. The condition in which all tuned circuits in a receiver follow accurately, throughout the tuning range, the frequency indicated by the tuning dial.
4. The motion given to the major lobe on an antenna so that a preassigned moving target in space is always contained within the major lobe.

Track on Jam–A method of passive target tracking using the jamming signal emitted by the target.

Track Telling–(DOD) The process of communicating air surveillance and tactical data information between command and control systems and facilities within the systems. Telling may be classified into the following areas:

a. *Back Tell*–The transfer of information from a higher to a lower echelon of command.

b. *Cross Tell*–The transfer of information between facilities at the same operational level.

c. *Forward Tell*–The transfer of information to a higher level of command.

d. *Lateral Tell*–see *Cross Tell.*

e. *Overlap Tell*–The transfer of information to an adjacent facility concerning tracks detected in the adjacent facilities' area of responsibility.

f. *Relateral Tell*–The relay of information between facilities through the use of a third facility. This type of telling is appropriate between automated facilities in a degraded communications environment.

Track while Scan–A method of target tracking which allows more than one target to be observed and tracked simultaneously. Systems using this technique do not change their antenna scan when acquiring the target.

Transceiver–(ASCC) A combined radio transmitter and receiver in which some circuits other than those of the power supply are common to both transmitter and receiver, and not providing for simultaneous transmission and reception.

Transponder–(DOD) A transmitter-receiver capable of accepting the electronic challenge of an interrogator and automatically transmitting an appropriate reply.

Ultra High Frequency–Frequencies in the band 300-3000 MHz.

Unintentional Radiation Exploitation–(DOD) Exploitation for operational purposes of non-information bearing elements of electromagnetic energy unintentionally emanated by targets of interest.

Unit Prefixes–The following prefixes are commonly used to indicate multiples or submultiples of scientific units.

Multiple	Prefix	Symbol
10^{12}	tera	T
10^{9}	giga	G
10^{6}	mega	M
10^{3}	kilo	k
10^{2}	hecto	h
10	deka	da
10^{-1}	deci	d
10^{-2}	centi	c
10^{-3}	milli	m
10^{-6}	micro	μ
10^{-9}	nano	n
10^{-12}	pico	p
10^{-15}	femto	f
10^{-18}	atto	a

Very High Frequency–Frequencies in the band 30-300 MHz.

Very High Frequency Omnirange–(ASCC) A radio aid which uses phase comparison of a ground transmitted signal to determine bearing.

Very Low Frequency–Frequencies in the band 3-30 kHz.

Video Frequency–(AF)
1. A band of frequencies extending from approximately 100 Hz to several MHz.
2. The frequency of the voltage resulting from television scanning. Range from 0 to 4 MHz or more.

WALLEYE–(AF) An air-to-surface homing glide weapon incorporating a contrast tracking television system for guidance and a high explosive linear shaped charge warhead. Designated as MK-1 Mod 0.

Warning Receiver (Electronic Warfare)–(AF) A receiver with the primary function of warning the user that his unit is being illuminated by an electromagnetic signal of interest.

Words per Minute–The usual measure of the speed of a teletype communications system.

ACRONYMS AND ABBREVIATIONS

AAA	Anti-Aircraft Artillery
AAM	Air-to-Air Missile
ACET	Automatic Cancellation of Extended Targets
ADA	Air Defense Artillery
ADF	Automatic Direction Finding
AEW	Airborne Early Warning
AF	Audio Frequency, Air Force
AFB	Air Force Base
AFC	Automatic Frequency Control
AGC	Automatic Gain Control
AI	Airborne Intercept
AJ	Anti-Jamming (see ECCM)
AM	Amplitude Modulation
ARDF	Airborne Radio Direction Finding
ARM	Anti-Radiation Missile
ASK	Amplitude Shift Keying
ASM	Air-to-Surface Missile
ATV	Automatic Threshold Variation
AVC	Automatic Volume Control (see AGC)
AVNL	Automatic Video Noise Limiting
AWACS	Airborne Warning and Control System
BFO	Beat Frequency Oscillator
BMEWS	Ballistic Missile Early Warning System
°C	Degree Centigrade (see Temperature Scales)
CAP	Combat Air Patrol
CEP	Circular Error Probable
CFAR	Constant False Alarm Rate
CHIRP	Linear Intra-pulse FM (see LIFMOP)
COHO	Coherent Oscillator
COMINT	Communications Intelligence
COMSEC	Communications Security
CONELRAD	Control of Electromagnetic Radiation
CRT	Cathode Ray Tube
CSC^2	Cosecant Squared
CW	Continuous Wave
dB	Decibel(s)
DBB	Detector Back Bias, Detector Balanced Bias
DC	Direct Current
DECM	Deceptive ECM (see Electronic Deception)
DF	Direction Finding
DME	Distance Measuring Equipment
DSB	Double Sideband

ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
EHF	Extremely High Frequency
ELINT	Electronic Intelligence
EMCON	Emission Control
EMP	Electromagnetic Pulse
EOB	Electronic Order of Battle
ER	Electronic Reconnaissance
ESM	Electronic Warfare Support Measures
EW	Electronic Warfare, Early Warning
EWO	Electronic Warfare Officer
°F	Degree Fahrenheit (see Temperature Scales)
FAGC	Fast AGC
FEBA	Forward Edge of the Battle Area
FC	Fire Control
FLIR	Forward Looking Infrared
FM	Frequency Modulation
FSK	Frequency Shift Keying
FTC	Fast Time Constant
GCI	Ground Controlled Intercept
GHz	Gigahertz (see Unit Prefixes)
HF	High Frequency (see Frequency Band Designations)
HOJ	Home on Jam
Hz	Hertz
IAGC	Instantaneous AGC
IF	Intermediate Frequency
IFC	Instantaneous Frequency Correlator
IFF	Identification, Friend or Foe
IFR	Instrument Flight Rules
IMC	Instrument Meterological Conditions
IR	Infrared
IRCM	Infrared Countermeasures
J/S	Jamming-to-Signal Ratio
°K	Degree Kelvin (see Temperature Scales)
kHz	Kilohertz (see Unit Prefixes)
KV	Kilovolts (see Unit Prefixes)
KW	Kilowatts (see Unit Prefixes)
LASER	Light Amplification by Stimulated Emission of Radiation
LF	Low Frequency (see Frequency Band Designations)
LIFMOP	Linearly Frequency Modulated Pulse
LLLTV	Low Light Level Television
LORAN	Long Range Navigation System
LORO	Lobe on Receive Only

LOS	Line of Sight
MA	Mission Accomplishment
MASER	Microwave Amplification by Stimulated Emission of Radiation
MC	Missile Control
MF	Medium Frequency (see Frequency Band Designations)
MHz	Megahertz (see Unit Prefixes)
MLC	Main Lobe Cancellation
MOPA	Master Oscillator Power Amplifier
MTI	Moving Target Indicator
NBFM	Narrow Band Frequency Modulation
OJT	On-the-Job Training
OTH	Over the Horizon
OTH-B	Over the Horizon–Backscatter
PAM	Pulse Amplitude Modulation
PCM	Pulse Code Modulation
PDM	Pulse Duration Modulation
PECM	Passive ECM
PIE	Pulse Interference Elimination
PLD	Pulse Length Discrimination (see PWD)
PM	Phase Modulation
PPI	Plan Position Indicator
PPM	Pulse Position Modulation
PPS	Pulses per Second
PRF	Pulse Repetition Frequency
PRI	Pulse Repetition Interval
PRT	Pulse Repetition Time
PSK	Phase Shift Keying
PW	Pulse Width
PWD	Pulse Width Discrimination
PWM	Pulse Width Modulation
QRC	Quick Reaction Capability
°R	Degree Rankine (see Temperature Scales)
RADAR	Radio Detection and Ranging
RAM	Radar Absorbing Material
RCS	Radar Cross Section
RDF	Radio Direction Finding (see Direction Finding)
RF	Radio Frequency
RFI	Radio Frequency Interference
RHAW	Radar Homing and Warning
RINT	Radiation Intelligence
ROB	Radar Order of Battle
ROC	Required Operational Capability
ROR	Range Only Radar
RPD	Random Pulse Discrimination
RPV	Remotely Piloted Vehicle

RWR	Radar Warning Receiver
SAM	Surface-to-Air Missile
SCAD	Supersonic Cruise Armed Decoy
Sec	Seconds
SHF	Super High Frequencies (see Frequency Band Designators)
SHORAN	Short Range Navigation System
SIF	Selective Identification Feature
SIGINT	Signal Intelligence
S/J	Signal-to-Jamming Ratio
SLAR	Side Looking Airborne Radar
SLS	Side Lobe Suppression
S/N	Signal-to-Noise Ratio
SOJ	Stand-Off Jamming
SORO	Scan on Receive Only
SSB	Single Sideband
SSJ	Self-Screening Jammer
SSSC	Single Sideband Suppressed Carrier
STC	Sensitivity Time Control
TA	Target Acquisition
TACAN	Tactical Air Navigation System
THz	Terahertz (see Unit Prefixes)
TOA	Time of Arrival
TOJ	Track on Jam
TRF	Tuned Radio Frequency
TTR	Target Tracking Radar
TV	Television
TWS	Track while Scan
TWT	Traveling Wave Tube
UHF	Ultra High Frequency (see Frequency Band Designations)
URE	Unintentional Radiation Exploitation
V	Volts
VFR	Visual Flight Rules
VHF	Very High Frequency (see Frequency Band Designations)
VLF	Very Low Frequency (see Frequency Band Designations)
VMC	Visual Meterological Conditions
VOR	VHF Omnirange
VSB	Vestigial Sideband
W	Watts
WBFM	Wideband Frequency Modulation
W/MHz	Watts per Megahertz
WPM	Words per Minute

INDEX

USAFA/USAF ACADEMY, CO/79-138